Wikiprint Book

Title: CTM-200 Command Reference

Subject: CTM-200 Documentation: Command Reference

Version:

Date: 2013-09-12

Table of Contents

accelcond r a [d] [l] [mt] 9
accelreport n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 10
accelsensor n 11
agpspde ip port tm pc pl nl 12
apn name 13
autoconnect n 14
autopevent n 15
aux dev name 16
aux lead c1 [c2] [c3] [c4] [c5] 17
aux leadterm m 18
aux len n 19
aux mode m 20
aux polldev name 21
aux polllen n 22
aux pollnow 23
aux pollstr str 24
aux polltim n [f] 25
aux report r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 26
aux reptim n 27
aux term c1 [c2] [c3] [c4] [c5] 28
boomreport r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 29
bt console n 30
bt enable n 31
bt locip ipaddr 32
bt locname name 33
bt locname pin 34
bt nap n 35
bt obd n 36
bt remname n name 37
bt rempin n pin 38
can apply 39
can enghours n 40
can engparam m 41
can odometer n 42
can prot p 43
can psthruid n id 44
can psthrumin n mt 45
can qryrate n 46
cardlistclear 47
cardlistload filename url [username] [passwd] 48
cardlistsave 49
cardlockload lock-script-file-name url [username] [passwd] 50
cardunlockload unlock-script-file-name url [username] [passwd] 51
clientmac nn:nn:nn:nn:nn:nn 52
confdrop 53
confupgrade script-name url [username] [passwd] 54
ctm15x 55
data [0] 56
datacond x 57
datareport r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 58
device cell type 59
device cellnetwork n 60
device cellnetwork n 61
device priority n 62
device wifi type 63
dir pppppppppp [qqqqqqqqqq] 64
dmz ip 65
dnscheck n 66
dout n x [d] 67

dyndns user password domain 68
emailsrv ip 69
enghours n 70
enghrmode n 71
esn 72
ethernet n 73
event add event_description [log-level] 74
event dump [-f N | -h N] [-l N | -t N] [-raw] [EVENT_FILTER] [email@address] 75
event healthinterval n 76
event logclear 77
event dump [-f or -h N] [-l or -t N] [-raw] [EVENT_FILTER] [email@address] 78
event loglevel min max 79
event minoffline n 81
eventreport r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 82
firewall n extport locport t ip s 83
freeconsole 84
friends n ip netmask [t] 85
ftp remote n 86
ftp server n 87
fuel io n x y z 88
fuel mode n 89
fuel query 90
fuel rate i d t 91
fuel rate query 92
fuel rate reset 93
fuel reset 94
geort acount 95
geort c2bin [-d] 96
geort delete route 97
geort enable n 98
geort list [n | -w] 99
geort period m 101
geort rcount 102
geort report r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 103
geort th r t 104
geort update r u [n] [p] 105
gopad n 106
gpsaccel n a [d] 107
gpsaddmes n m1 [m2] [m3] [m4] 108
gpscond n b t [d] [ms Ms] [h hs] [mt] 109
gpsdata 110
gpsdelmes n m 111
gpsdgps n 112
gpsemail n emailaddr 113
gpsgga 114
gpsinput m 115
gpslocip n ipaddr 116
gpslocport n port 117
gpsmes 118
gpsparam input priority port br db p sb fc 119
gpspos n ±xx.xxxxxx ±yyy.yyyyyy 120
gpsremip n iii.iii.iii.iii 121
gpsremport n xxxxx 122
gpsrep n l r s 123
gpsrmc 124
gpssms n ppppppppppemailaddr 125
gpstime n 126
idle cond n a b c 127
idle mode n 128
idle query 129
idle report n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 130
idle reset 131

idle time n 132
igncond n a 133
ignreport [n] [r1] [r2] [r3] [r4] [r5] [r6] [r7] [r8] 134
input 135
insetup n d x.x p a 136
ioaddmes n x [x2][x3][x4] 137
iocond n b t i1 i2 IP mt 138
iodelmes n x 139
ioemail n emailaddr 140
iolocip n iii.iii.iii.iii 141
iolocport n xxxxx 142
iomes 143
ioremip n iii.iii.iii.iii 144
ioremport n xxxxx 145
iorep n l r s 146
iosms n ppppppppppp|emailaddr 148
ipadr 149
ipsec 150
ipsec dpddelay n 151
ipsec dpdmaxfail n 152
ipsec dpdretry n 153
ipsec enable n 154
ipsec ikeauth psk 155
ipsec ikedhgroup n 156
ipsec ikeenc alg 157
ipsec ikeexchange mode 158
ipsec ikehash alg 159
ipsec ikeinitial n 160
ipsec ikelifetime n 161
ipsec ikemodecfg n 162
ipsec ikemyid type value 163
ipsec ikepassive n 164
ipsec ikepeerid type value 165
ipsec ikeproposal obey|strict|claim|exact 166
ipsec ikerekey on|off|force 167
ipsec ikeverifyid n 168
ipsec localnet n 169
ipsec loglevel info|notify|debug|debug2 170
ipsec natt n 171
ipsec nattkeepalive n 172
ipsec psk iii.iii.iii.iii key 173
ipsec rekey on|off|force 174
ipsec remgw iii.iii.iii.iii 175
ipsec remnet n iii.iii.iii.iii m 176
ipsec remping n 177
ipsec remtarget iii.iii.iii.iii 178
ipsec restrict n 179
ipsec saauth alg 180
ipsec saenc alg 181
ipsec salifetime n 182
ipsec sapfsgroup n 183
ipsec show 184
ipsec split n 185
lanbridge n 186
landhcp p ddd n 187
landns p iii.iii.iii.iii [jjj.jjj.jjj.jjj] 188
lanfriends n xx:xx:xx:xx:xx:xx 189
langw p iii.iii.iii.iii 190
lanip p iii.iii.iii.iii [mmm.mmm.mmm.mmm] 191
lannat p n 192
lannetmask p iii.iii.iii.iii 193
lanproto p type 194

lanrepip iii.iii.iii.iii 195
lanwdn 196
mbusm add n ip|serial 197
mbusm cond n b t [sid1, r1, dt1, md1, Md1] [sid2, r2, dt2, md2, Md2] [mt] 198
mbusm data n 200
mbusm del n 201
mbusm exccond e 202
mbusm excreport r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 203
mbusm poll n r c [dt] [f] [o] [e] 204
mbusm report n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 205
mip n 206
modbusadd id [ip|serial] 207
modbusctm130 n 208
modbusdel n 209
modbusgw 210
modbusidmap n ip p 211
modbusmode n 212
modbusport xxxxx 213
modbussecure n 214
mode a b c 215
modemid <string> 217
modemmode n 218
modemmodedhcp n 219
msgredirect add xxx.xxx.xxx.xxx yyyyy 220
msgredirect del xxx.xxx.xxx.xxx yyyyy 221
msgredirect enable n 222
msgredirect list 223
msgredirect port xxxxx 224
msgredirect remip xxx.xxx.xxx.xxx 225
multiwan enable n 226
multiwan mode m 227
netwd t n target p m 228
networktime n 229
nmeamode n 230
ntpserver url 231
ntptime n 232
obdcond n b t mt [trig1 ... trig4] 233
obddata 235
obdreport n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 236
obdsp n 237
odometer n 238
orientation n 239
otasp 241
pad 242
pad clientport port 243
pad echo n 244
pad esc str 245
pad esct n 246
pad fifo n 247
pad fwdc x r 248
pad fwdl x 249
pad fwdt t 250
pad ip ipaddr 251
pad mode x 252
pad pfc x 253
pad port p 254
pad reset 255
pad secure n 256
pad svct n [c] 257
panicreportack t 258
panicreport r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 259
panicreportack t 260

panicreptype m 261
pendantreport r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 262
pin n 263
ping n iii.iii.iii.iii|website 264
pobdx n1 [n2] [n3] [n4] [n5] [n6] [n7] [n8] 265
port n r d p s f 266
ppp 267
pswd n 268
pupcond n a 269
pupreport n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 270
pwr accelt a 271
pwr geofence lat lon rad mode 272
pwr mode n 273
pwr override m 274
pwr rtc u m 275
pwr sdwn a ddddd 276
pwr speedth s t 277
pwr temp l h m 278
pwr vcct vv.v t 279
pwr woe m t1 t2 t3 f 280
ratesel n 282
ratetmr n 283
repaddmes n x [x2][x3][x4] 284
repdelmes n x 285
repemail n emailaddr 286
repfiledelivery n t rt username server-path port 287
repfiledir local-path 288
repfilename n name 289
repfileout local-path 290
repfilesize kb 291
repfiletimestamp n 292
repfilezip c 293
replocip n iii.iii.iii.iii 294
replocport n xxxxx 295
reportscripts n 296
repremip n iii.iii.iii.iii 297
repremport n xxxxx 298
repsms n ppppppppppp|emailaddr 299
reptype n l r s 300
rfon 302
rfstats 303
rfswitch x 304
rmtssh n 305
rmttelnet 306
rmtweb n 307
rssi 308
saltreport r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] 309
sat enable n 310
sat flush 311
sat force n 312
sat ip iii.iii.iii.iii 313
sat mt n 314
sat port xxxxx 315
sat pwr n 316
sat reset 317
sat stats 318
satbackup b bt g gt o 319
cmd save 320
sendreport n x [x2][x3][x4] 321
showconfig [-quiet emailaddr] 322
showstate 323
sms enable n 324

sms friends n ppppppppppp **325**
sms fwdreport r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] **326**
smssend **327**
smstext string delimiter **328**
smsto ppppppppppp **329**
smsview **330**
snfdelay t rssi **331**
snfflush **332**
snflog n | all **333**
snfonsd n **334**
snmp n **335**
spc nnnnnn **336**
speedth s t **337**
sshkey dss | rsa **338**
sshport port **339**
sshtimeout n **340**
stm upgrade f [u] [n] [p] **341**
swipegpio n **342**
swipeid **343**
swipemode n **344**
swipereport r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] **345**
syslog n **346**
taipchecksum n **347**
taipid DDDD **348**
taipuseid n **349**
tcppersist n **350**
telnetport n **351**
telnetpswd n **352**
telnettimeout n **353**
timesync t **354**
timezone tz **355**
universal n **356**
univwd m url/report **357**
univwdtimer n p **358**
upgradefw imagefile.tar url username passwd **359**
upgradesrv a.a.a.a **360**
usepeerdns n **361**
user name **362**
vcc **363**
vcccond n o [a.a] [mt] **364**
vccreport n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8] **365**
ver **366**
vpnc n **367**
vue ack string **368**
vue period n **369**
vue port n **370**
vue pwrup n **371**
vue remip a.a.a.a **372**
vue remport n **373**
vue service n **374**
wifi ap|client channel n **375**
wifi ap|client country country-code **376**
wifi ap|client encryption enctype **377**
wifi ap|client hwmode mode **378**
wifi ap|client key pre-shared-key **379**
wifi mac **380**
wifi radiusport n **381**
wifi radiusserver iii.iii.iii.iii **382**
wifi ap|client ssid SSID **383**
wifi watchdog n [t] **384**
wlan dns ipaddr **385**
wlan enable n **386**

wlan gw ipaddr **387**
wlan ip ipaddr **388**
wlan netmask iii.iii.iii.iii **389**
wlan proto type **390**
wpan acktype type **391**
wpan adddev xx-xx-xx-xx-xx-xx-xx-xx **392**
wpan delall **393**
wpan deldev xx-xx-xx-xx-xx-xx-xx-xx **394**
wpan dist n **395**
wpan panid xxxx **396**
wpan pensrv x yyyy **397**
wpan secure n **398**
wpan stm n **399**
wpanpanid xxxx **400**

accelcond *r a [d] [l] [mt]*

Set acceleration trigger condition.

r = 1 to 8	Acceleration report number
a = 0	Longitudinal acceleration disabled (**Default**)
a > 0	Longitudinal acceleration threshold in km/h/s (Must be positive)
d = 0	Longitudinal deceleration (braking) disabled (**Default**)
d < 0	Longitudinal deceleration threshold in km/h/s (Must be negative)
l = 0	Lateral acceleration disabled (**Default**)
l > 0	Lateral acceleration threshold in km/h/s (Must be positive)
mt = 0 to 65535	Minimum time between reports in seconds (**Default 0**)

Notes:

A report is triggered when one of the following conditions applies:

- acceleration > **a**
- acceleration < **d**
- abs(lateral acceleration) > **l**

Examples:

1. Trigger on hard acceleration only when longitudinal acceleration exceeds **15** km/h/s :
   cmd accelcond 1 15 0 0
1. Trigger on hard braking only when longitudinal deceleration exceeds **-20** km/h/s :
   cmd accelcond 1 0 -20 0
1. Trigger on hard acceleration when longitudinal acceleration exceeds **15** km/h/s OR braking when longitudinal deceleration exceeds **-20** km/h/s :
   cmd accelcond 1 15 -20 0
1. Trigger on hard turning only when lateral acceleration exceeds **35** km/h/s :
   cmd accelcond 1 0 0 35
1. Set a minimum timeout of **30**s between reports :
   cmd accelcond 1 0 0 35 30

See also: [Acceleration]

Firmware revision 2.0.3.2255-80

accelreport *n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for an acceleration triggered report.

n = 1 to 8	Acceleration trigger condition
r1 to r8 = 0	Disables the report (**Default**)
r1 to r8 = 1 to 999	Report number

Notes:

- For **accelreport** to function properly when **accelsensor 1** is set, the CTM must be configured using the commands **accelcond**, **accelsensor**, and **orientation**.

Example:

1. Set reports #2 and #100 for acceleration triggered report #1 :
   cmd accelreport 1 2 100

See also: [Acceleration]

Firmware revision 2.0.3.2255-80

accelsensor *n*

Specify a sensor to use for report triggering on longitudinal acceleration.

n = 0	Use accelerometer (**Default**)
n = 1	Use GPS

Notes:

- The accelerometer sensor is always used for lateral acceleration triggering/reporting.
- With **n = 0**, both acceleration trigger and $PACCEL use the accelerometer sensor. GPS speed sensor is used for $PACCEL2 message.
- With **n = 1**, both acceleration trigger and $PACCEL use the GPS speed sensor. Accelerometer sensor is used for $PACCEL2 message.

Examples:

1. Use GPS to obtain longitudinal acceleration values :
   cmd accelsensor 1

See also: [Acceleration]

Firmware revision 2.0.3.2255-80

agpspde *ip port tm pc pl nl*

This command is used to configure Assisted GPS (A-GPS) parameters on supported wireless data cards/modules.

The cellular device chipset contains a GPS receiver. Position Determine Equipment (PDE) assists the cellular device to speed up satellite acquisition, the PDE sends satellite almanac and ephemeris information to the device.

ip = 0.0.0.0 to 255.255.255.255	IP address for location processing (**Default 216.198.139.92**)
port = 0 to 65535	Port number for location processing (**Default 8889**)
tm = 0	Transport mechanism is TCP/IP (**Default**)
tm = 1	Transport mechanism is Data Burst
pc	Position calculation type, fix type
pc = 1	Standalone
pc = 2	MS-based only
pc = 3	MS-assisted only = A-GPS Only (**Default**)
pc = 4	Optimum speed
pc = 5	Optimum accuracy
pc = 6	Optimum data
pl	Privacy level for location processing
pl = 0	Low (**Default**)
pl = 1	Medium
pl = 2	High
nl	Network access level for location processing
nl = 0	Network access only
nl = 1	No network access
nl = 2	Network access with demodulation (**Default**)
nl = 3	Network access without demodulation

Notes:

- This feature currently works **only** on later model Sierra Wireless data devices that support A-GPS (USB598, USB597).
- When a later model Sierra Wireless data device is used with a modem configured in half bridge mode, A-GPS support is not available and must be disabled.
- A-GPS is disabled by **cmd agpspde 0.0.0.0 0 0 1 0 1**

Examples:

1. Set A-GPS parameters :
   cmd agpspde 124.105.114.86 5412 0 3 0 2
1. Disable A-GPS feature :
   cmd agpspde 0.0.0.0 0 0 1 0 1

Firmware revision 1.2.2 (rev 1531)

apn *name*

This command configures the APN(Access Point Name) for a modem.

name	Carrier Access Point Name (APN), eg. isp.telus.com, inet.bell.ca

Notes:

- This command is only applicable to GSM/GPRS/HSPA devices.
- more info about access point name can be found at ?http://en.wikipedia.org/wiki/Access_Point_Name

---

Examples:

1. Set APN to new.apn.com :
   cmd apn new.apn.com

See also: [Cellular]

Firmware revision 1.2.0_RC7 (rev 1187)

autoconnect *n*

Configure the modem to automatically connect to a network.

n = 0	Manual network connection
n = 1	Auto network connection (**Default**)

Examples:

1. Set the modem to automatically connect to a wireless service :
   cmd autoconnect 1

See also: [Cellular]

Firmware revision 2.0.0.2125

autopevent *n*

Enables the [$PEVENT] message to be pre-pended to any existing reports. The [$PEVENT] message contains trigger or event that generated the report.

n = 0	Disable [$PEVENT] message (**Default**)
n = 1	Enable [$PEVENT] message

Examples:

1. Enable autopevent :
   cmd autopevent 1

See also: [Reports]

Firmware revision 2.0.4.2520

aux dev *name*

This command sets the auxiliary device name that will be sent as part of the message when in [mode 23/24].

name = string (max 4 chars)	Device name (**Default AUX1**)

Examples:

1. Sets the auxiliary device name to be "TDev" :
   cmd aux dev TDev

See also: [Salt Reports]

Firmware revision 2.0.5.3358

aux lead *c1 [c2] [c3] [c4] [c5]*

This command sets the leading characters for [mode 24], auxiliary interface.

c1 to c5	Hex format (**Default 0D 0A**)

Notes:

- The leading characters are forwarded in mode 24

Examples:

1. Set the leading character to be 0x0D :
   cmd aux term 0D
1. Set the leading characters to be <CR><LF> :
   cmd aux term 0d 0a
1. Set the leading characters to be "START" :
   cmd aux term 53 54 41 52 54

See also: [Auxiliary Reports]

Firmware revision 2.0.5.3358

aux leadterm *m*

This command sets whether to use leading characters, terminating characters or both for [mode 24].

m=0	Don't use leading or terminating characters (**Default**)
m=1	Use leading characters
m=2	Use terminating characters
m=3	Use leading and terminating characters

Examples:

1. Set to use leading characters :
   cmd aux leadterm 1

See also: [Auxiliary Reports]

Firmware revision 2.0.5.3358

aux len *n*

This command sets the amount of bytes to read for [mode 23/24].

n = 0 to 205	Bytes to read, must be greater than 0 for mode 23 to work (**Default 205**)

Notes:

- For mode 23, responses greater than the configured length will be split over multiple packets
- For mode 24, responses are truncated at a maximum length of 205
- For mode 24, length includes leading and terminating bytes and works as below with aux mode 0:

cmd aux leadterm	Description
1	Returns n bytes, starting with leading chars
2	Returns n bytes from the end, ending with terminating chars
3	Once n bytes or more have been reached, return msg starting with leading chars and ending with terminating chars

---

Examples:

1. Set the bytes to read to 88 for CS-440 device :
   cmd aux len 88

See also: [Salt Reports]

Firmware revision 2.0.5.3358

aux mode *m*

Set the processing mode for [mode 23/24].

m=0	Disables any processing, send raw data (**Default**)
m=1	Parker - Send each msg when received
m=2	Parker - Send on change msgs when received; cache periodic msgs and send them at configured interval (cmd aux reptime)
m=3	Parker - Cache on change and periodic msgs and send them at configured interval (cmd aux reptime)

Examples:

1. Process the incoming Parker message and send the processed result immediately :
   cmd aux mode 1

See also: [Salt Reports]

Firmware revision 2.0.5.3358

aux polldev *name*

Note: Should use aux dev if using FW 2.0.5.3358 or higher

This command sets the auxiliary device name that will be sent as part of the message when in [mode 23].

name = string (max 4 chars)	Device name (**Default AUX1**)

Examples:

1. Sets the auxiliary device name to be "TDev" :
   cmd aux polldev TDev

See also: [Salt Reports]

Firmware revision 2.0.5.3101

aux polllen *n*

Note: Should use aux len if using FW 2.0.5.3358 or higher

This command sets the amount of bytes to read for [mode 23] (Generic auxiliary interface).
Responses greater than the configured length will be split over multiple packets.

n = 0 to 205	Bytes to read, must be greater than 0 for mode 23 to work (**Default 205**)

Examples:

1. Set the bytes to read to 88 for CS-440 device :
   cmd aux polllen 88

See also: [Salt Reports]

Firmware revision 2.0.5.3101

aux pollnow

This command tells CTM to poll/listen to the auxiliary device when in [mode 23].

Examples:

1. To poll the auxiliary device :
   cmd aux pollnow

See also: [Salt Reports]

Firmware revision 2.0.5.3101

aux pollstr *str*

This command sets the polling string that is sent if configured when **cmd aux pollnow** is executed when in [mode 23].

str = string (max 20 chars)	Polling string (**Default blank**)
str = auxpollstr.txt	Use polling commands stored in auxpollstr.txt

Notes:

- If using `auxpollstr.txt`, the file must be located in `/var/config` before this command is set.

Examples:

1. Sets the polling string to be "@1" for CS-440 device :
   cmd aux pollstr @1
1. Configure to use a list of polling commands for Dickey John device :
   cmd aux pollstr auxpollstr.txt

See also: [Salt Reports]

Firmware revision 2.0.5.3101

aux polltim *n [f]*

This command sets the timeout for each polling command when polling in [mode 23].
In [mode 23], a message without the payload will still be sent, even if nothing was received (delimiters and auxiliary device name will still be sent.)

n = 0 to 30000	Timeout in 10ms increments (**Default 400**)
f = 0 or 1	Timeout enforced (**Default 0**)

Notes:

- If timeout is enforced (`f=1`), a device will time out after the specified time
- If `f=0`, a device is timed out when the time since last received byte is greater than the configured aux polltim

---

Examples:

1. Set the timeout for the CS-440 device (4s) :
   cmd aux polltim 400
1. Set the timeout for the Dickey John device (200ms) :
   cmd aux polltim 20 1

See also: [Salt Reports]

Firmware revision 2.0.5.3101

aux report *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for auxiliary interface triggered reports.

r1 to r8 = 0	Disables the report (**Default**)
r1 to r8 = 1 to 999	Report number

Notes:

- When aux report is configured to use a report, it appends a modified message [114, $PGPS] to the already existing messages configured in the report. The appended message contains the frame data received on the serial port at the end of the default $PGPS message.

Examples:

1. Configure auxiliary interface triggered reports to use general report 1 :
   cmd aux report 1 0 0 0 0 0 0 0

See also: [Auxiliary Reports]

Firmware revision 2.0.5.2863

aux reptim *n*

This command sets the reporting frequency when in [mode 23/24].

n = 0	Send report when data received (**Default**)
n = 1 to 65535	Send report every n seconds

Examples:

1. Send a report every 60s:
   cmd aux reptime 60

See also: [Salt Reports]

Firmware revision 2.0.5.3358

aux term *c1 [c2] [c3] [c4] [c5]*

This command sets the termination characters for [mode 22/24], auxiliary interface.

c1 to c5	Hex format (**Default 0D 0A**)

Notes:

- The termination characters would not be forwarded by auxiliary interface triggered reports in mode 22
- The termination characters are forwarded in mode 24 (FW 2.0.5.3358)

Examples:

1. Set the termination character to be 0x0D :
   cmd aux term 0D
1. Set the termination characters to be <CR><LF> :
   cmd aux term 0d 0a
1. Set the termination characters to be "STOP" :
   cmd aux term 53 54 4f 50

See also: [Auxiliary Reports]

Firmware revision 2.0.5.2863

boomreport *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for boom-tracker triggered reports.

r1 to r8 = 0	Disables the report (**Default**)
r1 to r8 = 1 to 999	Report number

Notes:

- Requires [cmd mode 10] to be configured.

Examples:

1. Use general report 2 for boom-tracker triggered reports :
   cmd boomreport 2
2. Use general reports 1, 2 and 4 for boom-tracker triggered reports :
   cmd boomreport 1 2 4
3. Disable boom-tracker triggered reports :
   cmd boomreport 0

See also: [Boom Reports]

---

bt console *n*

Enables/disables Bluetooth console mode.

n = 0	Disable Bluetooth console mode (**Default**)
n = 1	Enable Bluetooth console mode

Notes:

- **cmd bt enable 1** must be set to use this feature

Examples:

1. Enable Bluetooth console :
   cmd bt console 1

See also: [Bluetooth]

Firmware revision 2.0.5.2959

bt enable *n*

Enables/disables Bluetooth Dongle.

n = 0	Disable Bluetooth function (**Default**)
n = 1	Enable Bluetooth function

Notes:

- Bluetooth console/NAP/OBD mode can only be used with **cmd bt enable 1**

Examples:

1. enable bluetooth dongle functionality :
   cmd bt enable 1

See also: [Bluetooth]

Firmware revision 2.0.5.2959

bt locip *ipaddr*

Sets the Bluetooth NAP IP address of bnep0 port.

ipaddr = 0.0.0.0 to 255.255.255.255	Bluetooth NAP IP address in decimal (**Default 0.0.0.0**)

Notes:

- This command should be used with **cmd bt enable 1** and **cmd bt nap 1**.

Examples:

1. Set the Bluetooth NAP IP address of bnep0 to 192.168.3.1 :
   cmd bt locip 192.168.3.1

See also: [Bluetooth]

Firmware revision 2.0.5.2959

bt locname *name*

Sets the local Bluetooth device name. The remote Bluetooth device should search this device name if the remote device tries to connect to CTM via Bluetooth.

name = string (max 20 chars)	Bluetooth local device name (**Default 0**)

Example:

1. Set the local Bluetooth device name as ?CTM200? :
   cmd bt locname CTM200

See also: [Bluetooth]

Firmware revision 2.0.5.2959

bt locname *pin*

Sets the local Bluetooth device password. The remote Bluetooth device should use this password when the remote device connects to CTM through the Bluetooth device.

pin = string (max 16 chars)	Bluetooth local device password (**Default 0**)

Examples:

1. Set the local Bluetooth device password as ?cypress? :
   cmd bt locpin cypress

See also: [Bluetooth]

Firmware revision 2.0.5.2959

bt nap *n*

Enables/disables Bluetooth Network Access Point mode. A NAP can act as a bridge between Bluetooth network and WWAN network on the CTM. This will allow a remote PC to access the Internet via Bluetooth.

n = 0	Disable Bluetooth NAP mode (**Default**)
n = 1	Enable Bluetooth NAP mode

Notes:

- Bluetooth NAP mode should be used with **cmd bt enable 1**.

Example:

1. Enable Bluetooth NAP :
   cmd bt nap 1

See also: [Bluetooth]

Firmware revision 2.0.5.2959

bt obd *n*

Enables/disables Bluetooth OBD mode.

n = 0	Disable Bluetooth OBD mode (**Default**)
n = 1 to 8	Enable Bluetooth OBD mode and use remname/rempin pair 1-8 for OBD polling

Notes:

- Bluetooth OBD mode should be used with **cmd bt enable 1**.
- In order to use J1939 protocol, **cmd obdsp 10** should be used.

Example:

1. Enable Bluetooth OBD and use the remote Bluetooth device 2 :
   cmd bt obd 2

See also: [Bluetooth]

Firmware revision 2.0.5.2959

bt remname *n name*

Sets the remote Bluetooth device name to search for when pairing with remote Bluetooth device.

n = 1 to 8	Device number
name = string (max 20 chars)	Remote Bluetooth device name (**Default 0**)

Examples:

1. CTM will be paired with a remote device with the name 'REMOTE1', and set it as device 2 :
   cmd bt remname 2 REMOTE1

See also: [Bluetooth]

Firmware revision 2.0.5.2959

bt rempin *n pin*

Sets the remote Bluetooth device password to use to pair with the remote device defined in **bt remname**.

n = 1 to 8	Device number that corresponds with device number in **bt remname**
pin = string (max 16 chars)	Bluetooth device password (**Default 0**)

Examples:

1. Use 'cypress' for the password to connect the remote Bluetooth device 2 :
   cmd bt rempin 2 cypress

See also: [Bluetooth]

Firmware revision 2.0.5.2959

can apply

Force re-configuration of STM with values set in [cmd can engparam] and [cmd can prot].

Examples:

1. Configure a CAN command :
   cmd can engparam ffffe
   Force STM re-configuration :
   cmd can apply

See also: [Vehicle Support]

Firmware revision 2.0.3.2330

can enghours *n*

Determines the source of engine hours value returned by **cmd enghours**. If enghrmode is not 0, this command is ignored.

n = 0	Disabled (**Default**)
n = 1	Engine hours from J1939 only

See also: [Engine Diagnostics Support]

Firmware revision 2.0.5.3003

can engparam *m*

Defines which parameters are to be queried/reported.

m	Hexadecimal bit mask
bit = 0	Not used
bit = 1 to 127	p1 to p127 respectively (**Default FFFFFFFFFFFFFFFFFFFFFFFFFFFFFE**)

Examples:

1. Enable p1 and p52 :
   cmd can engparam 10000000000002

See also: [Vehicle Support], [OBD2/J1939 Parameters Table]

Firmware revision 2.0.3.2330

can odometer *n*

Determines the source of odometer value returned by **cmd odometer**.

n = 0	Odometer calculated by CTM based on GPS data (**Default**)
n = 1	Odometer from OBD2/J1939 only
n = 2	Odometer from OBD2/J1939 if available, otherwise calculated based on GPS data

---

See also: [Engine Diagnostics Support], [GPS Configuration]

Firmware revision 2.0.5.3003

can prot *p*

Enables/disables internal CAN and sets the protocol to be used as follows:

p = 0	CAN disabled (**Default**)
p = 1	ISO15765-4
p = 2	J1939

Examples:

1. Selects ISO15765-4 :
   cmd can prot 1

See also: [Vehicle Support], [OBD2/J1939 Parameters Table]

Firmware revision 2.0.3.2330

can psthruid *n id*

Configure specific CAN header/ID to look for (J1939/OBD2) when using canpsthru ps.

n = 1 to 8	Support up to 8 IDs
id = 8 bytes max	ID to look for, 0 to disable (**Default 0**)

Examples:

1. Look for FEF1 coming from source address 0x00 and 0x31 :
   cmd can pasthruid 1 18FEF100
   cmd can pasthruid 2 18FEF131

See also: [Vehicle Support]

Firmware revision 2.0.5.3187

can psthrumin *n mt*

Minimum time between CAN data for a specific header/ID when using canpsthru ps. If mt is not reached, data for that header/ID is discarded.

n = 1 to 8	Support up to 8 IDs
mt = 0 to 655	Minimum time between CAN data in 100ms increment (**Default 1**)

Examples:

1. Limit the first ID to be reported every 200ms and second ID every 500ms :
   cmd can pasthrumin 1 2
   cmd can pasthrumin 2 5

See also: [Vehicle Support]

Firmware revision 2.0.5.3187

can qryrate *n*

Sets the maximum querying rate for OBD.

n = 0 to 18000	Querying rate in 100ms units (**Default 2**)

Examples:

1. Limit the querying rate to one query a second :
   cmd can qryrate 600

See also: [Vehicle Support]

Firmware revision 2.0.5.3187

cardlistclear

Removes list of approved swipe-card IDs from modem.

Examples:

1. **cmd cardlistclear**

See also: [RFID Card Reader Support]

Firmware revision 1.2.1

cardlistload *filename url [username] [passwd]*

This loads the approved ID list used with the swipe card interface from a remote location (FTP/HTTP server). The approved ID list file is copied to **/var/config/approved.txt**

filename	Name of the approved ID list to load onto the modem
url	Address of the FTP or HTTP server, can also be an IP address, prefixed by ftp:// or http:// respectively. If no prefix is specified (eg. cypress.bc.ca) then ftp:// is used.
username	Username to access FTP server (ignored when **url** is prefixed by http://)
passwd	Password to access FTP server (ignored when **url** is prefixed by http://)

Notes:

- The command requires 4 parameters when accessing an FTP server or 2 parameters when accessing an HTTP server.
- The approved ID list is a text file containing approved swipe card IDs.
- Each line in the approved ID list can only contain one 16-character ID (HHHHHHHHHHHHHHHH) for iButton or an ID of the format NNNNN or NNN-NNNNN for Wiegand (where H=0-F or X for wildcard, and where N=0-9 or X for wildcard).
- Each line must be terminated by a UNIX line ending (0x0A or <LF>).
- IDs must be in upper case.
- The list must be saved with **cardlistsave**, which will also convert IDs of format NNN to XXX-NNNNN
- Wildcards can be used to allow batches of IDs.

  For example:

```
XXX-12345        - allow card ID 12345 and ignore facility code
12345            - allow card ID 12345 and ignore facility code
039-XXXXX        - allow all cards from facility code 039
XXX-12XXX        - allow all cards with ID that begins with 12--- and ignore facility code
xxxxxxxxxxxxxx01 - allow all ibuttons with family code 01
```

Examples:

1. Where *new-approved.txt* is the approved ID list, *cypress.bc.ca* is the FTP server, *guest* is the username of the FTP server and *guestpw* is the password of the FTP server :
   cmd cardlistload new-approved.txt cypress.bc.ca guest guestpw
1. Where *new-approved.txt* is the approved ID list, and *cypress.bc.ca* is the HTTP server :
   cmd cardlistload new-approved.txt http://cypress.bc.ca

See also: [RFID Card Reader Support]

Firmware revision 1.2.1 and 2.0.5.3067

cardlistsave

Process and store a list of approved swipe-card IDs for use by CTM and bootloader swipe card reader application.

Notes:

- A list of approved IDs must first be loaded to the modem using [cardlistload].

Examples:

1. **cmd cardlistsave**

See also: [RFID Card Reader Support]

Firmware revision 1.2.1 and 2.0.5.3067

cardlockload *lock-script-file-name url [username] [passwd]*

This command is used to load the custom lock script associated with the swipe card interface.

lock-script-file-name	Name of the lock script file
url	Address of the FTP or HTTP server, can also be an IP address, prefixed by ftp:// or http:// respectively If no prefix is specified (eg. cypress.bc.ca) then ftp:// is used
username	Username to access FTP server (ignored when **url** is prefixed by http://)
passwd	Password to access FTP server (ignored when **url** is prefixed by http://)

Notes:

- The command requires 4 parameters when accessing an FTP server or 2 parameters when accessing an HTTP server.

Examples:

1. Where *lock.sh* is the lock script, *cypress.bc.ca* is the FTP server, *guest* is the username of the FTP server and *guestpw* is the password of the FTP server :
   cmd cardlockload lock.sh cypress.bc.ca guest guestpw
1. Where *lock.sh* is the lock script, and *cypress.bc.ca* is the HTTP server :
   cmd cardlockload lock.sh http://cypress.bc.ca

See also: [RFID Card Reader Support]

Firmware revision 1.2.1

cardunlockload *unlock-script-file-name url [username] [passwd]*

This command is used to load the custom unlock script associated with the swipe card interface.

The command requires 4 parameters when accessing an FTP server or 2 parameters when accessing an HTTP server:

unlock-script-file-name	Name of the unlock script file
url	Address of the FTP or HTTP server, can also be an IP address, prefixed by ftp:// or http:// respectively If no prefix is specified (eg. cypress.bc.ca) then ftp:// is used
username	Username to access FTP server (ignored when **url** is prefixed by http://)
passwd	Password to access FTP server (ignored when **url** is prefixed by http://)

Examples:

1. Where *unlock.sh* is the unlock script, *cypress.bc.ca* is the FTP server, *guest* is the username of the FTP server and *guestpw* is the password of the FTP server :
   cmd cardunlockload unlock.sh cypress.bc.ca guest guestpw
1. Where *unlock.sh* is the unlock script, and *cypress.bc.ca* is the HTTP server :
   cmd cardunlockload unlock.sh http://cypress.bc.ca

See also: [RFID Card Reader Support]

Firmware revision 1.2.1

clientmac *nn:nn:nn:nn:nn:nn*

Use clientmac to set the 12-digit hexadecimal MAC address of a client computer Ethernet interface, if using modem mode (half-bridge mode) and DHCP.

Examples:

1. Set client MAC address :
   cmd clientmac 00:a0:d1:69:b2:c8

See also: [Half Bridge]

confdrop

When used, this command will look for the following configuration file: **/tmp/ctm200-config.tgz**

Notes:

- All previous command configuration will be overwritten by the contents of **ctm200-config.tgz**
- The firmware revision of the CTM-200(s) applying AND dropping the config must be identical.
- A powercycle ([cmd pwr mode 2]) is required for this command to take effect.

Examples:

1. Save the configuration on a CTM-200 (this will create */tmp/ctm200-config.tgz*) :
   cmd modemid CYPRESS
   cmd save
   Copy the *ctm200-config.tgz* file created in Example 1 to another CTM-200's */tmp* directory, and run the following command :
   cmd confdrop
   cmd pwr mode 2

```
/ # cmd modemid
cmd modemid CYPRESS
```

See also: [Device Management], [save]

Firmware revision 2.0.5.3015

---

confupgrade *script-name url [username] [passwd]*

Configures the modem for over-the-air configuration by means of a custom configuration script retrieved from a defined FTP or HTTP server.

script-name	Name of the configuration script to fetch/run
url	Can be **localhost**, or the address of the FTP or HTTP server, can also be an IP address, prefixed by ftp:// or http:// respectively If no prefix is specified (eg. cypress.bc.ca) then ftp:// is used
username	Username to access FTP server (ignored when **url** is prefixed by http:// or localhost://, or **url** is **localhost**)
passwd	Password to access FTP server (ignored when **url** is prefixed by http:// or localhost://, or **url** is **localhost**)

Notes:

- The command requires 4 parameters when accessing an FTP server, 2 parameters when accessing an HTTP server, or 2 parameters when accessing scripts locally.
- When **localhost** is specified as the **url**, the script file and its corresponding .md5 file must be located in **/etc/config** on the modem.
- Likewise, when **?localhost://tmp** is specified as the **url**, the script file and its corresponding .md5 file must be located in **/tmp** on the modem.
- The script file is a text file containing modem commands used to configure a modem. The script file must have UNIX line endings.

  Example script file

```
cmd mode 2
cmd gpsrep 1 0 3
cmd gpscond 1 1 30
cmd gpsremip 1 123.123.123.123
cmd gpsremport 1 5005
......
....
..
```

Examples:

1. Where *ctm15x-config.sh* is the script file, *cypress.bc.ca* is the FTP server, *guest* is the username of the FTP server, and *guestpw* is the password of the FTP server :
   cmd confupgrade ctm15x-config.sh cypress.bc.ca guest guestpw
1. Where *ctm15x-config.sh* is the script file, and *cypress.bc.ca* is the HTTP server :
   cmd confupgrade ctm15x-config.sh http://cypress.bc.ca
1. Execute the script */tmp/action.sh* on the modem :
   cmd confupgrade action.sh localhost://tmp
1. Execute the script */etc/config/action.sh* on the modem :
   cmd confupgrade action.sh localhost

See also: [Device Management]

Firmware revision 1.1.32

ctm15x

This command is used to enable a reset of protected configuration values.
Current protected configuration commands are:

- cmd data
- cmd eepromclear
- cmd eepromread
- cmd enghours
- cmd ethernet
- cmd odometer
- cmd rfswitch

Notes:

- cmd ctm15x must be run once prior to setting any of the above configuration values.
- cmd ctm15x is volatile and cannot be saved, its state will be reset following a modem power cycle or reboot

---

See also: [data], [eepromclear], [eepromread], [enghours], [ethernet], [odometer], [rfswitch]

Firmware revision 1.2.1 (1380)

data [0]

This command keeps track of the amount of data transmitted and received over the wireless data link.

Notes:

- **cmd factory** does not reset the counter to 0

Examples:

1. Reset the link data count to zero :
   cmd ctm15x
   cmd data 0
1. Query the current link data count (result shown in Megabytes) :
   cmd data

See also: [Wireless Networks]

Firmware revision 1.2.2

datacond *x*

This command is used to set the condition that will trigger wireless link data count report(s). Report(s) are sent whenever the total amount of data transmitted and received is a multiple of a specified amount.

x = 0	Disables the condition
x = 1 to 1999999	Total data amount in MB used for periodic triggering (**Default 10**)

Examples:

1. Set trigger when 5 MB total data has been transferred (i.e. 1 MB of data was transmitted and 4 MB of data was received) :
   cmd datacond 5

See also: [Data Reports]

Firmware revision 1.2.2

datareport *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for link data count triggered events.

r = 0	Disables the report (**Default**)
r = 1 to 999	Report number

Examples:

1. Use general report 1, 2 and 4 for link data count triggered reports :
   cmd datareport 1 2 4

See also: [Data Reports], [General Reports]

Firmware revision 1.2.2

device cell *type*

Configure the wireless cellular data device used by the CTM.

Notes:

- Default = **NONE**

Examples:

1. Configure the CTM to use the AC306 wireless data device :
   cmd device cell AC306
1. Configure the CTM to use the F5521E wireless data device :
   cmd device cell F5521E

See also: [Cellular]

Firmware revision 2.0.1.2225

device cellnetwork n

Configure cell device to use a specified network type.

Note:
This command is only supported on the following cell devices: Huawei E397B, Sierra Wireless AC313/320/330

n=DEFAULT use network type already set on the cell device (default)

n=AUTO automatically set the network type based on network availability

n=GSM GSM is the network type

n=HSPA HSPA is the network type

n=LTE LTE is the network type

This command requires a [cmd save] and a power cycle to take effect.

Examples:

1. Configure a supported cell device to use HSPA only

```
cmd device cellnetwork HSPA
cmd save
cmd pwr mode 2
```

1. Configure a supported cell device to automatically select its network type

```
cmd device cellnetwork AUTO
cmd save
cmd pwr mode 2
```

See also: [[device_cell device cell]

Verified command operation in openctm r2.0.5.3016

device cellnetwork *n*

Configure cell device to use a specified network type.

n = DEFAULT	Use network type already set on the cell device (**Default**)
n = AUTO	Automatically set the network type based on network availability
n = GSM	GSM is the network type
n = EVDO	EVDO is the network type (Huawei UML397 only)
n = HSPA	HSPA is the network type
n = LTE	LTE is the network type

Notes:

- This command is only supported on the following cell devices: Huawei E397B/UML397, Sierra Wireless AC313/320/330
- **EVDO** network type is only supported on the Huawei UML397
- **GSM** and **HSPA** network types are not supported on the Huawei UML397

Examples:

1. Configure a supported cell device to use HSPA only :
   cmd device cellnetwork HSPA
1. Configure a supported cell device to automatically select its network type :
   cmd device cellnetwork AUTO

See also: [Cellular]

Firmware revision 2.0.5.3257

device priority *n*

A CTM configured for dual-mode (cell + wifi client, or **cmd wlanenable 1**), also requires a specification of the preferred WAN interface.

n = wifi	Wifi is the priority device (**Default**)
n = cell	Cellular is the priority device

Notes:

In a dual-mode cell + wifi client setup, where **wifi** is the priority device:

- default route is set to wifi gateway
- if wifi is not online, the cell interface will be the default route.

In a dual-mode cell + wifi client setup, where **cell** is the priority device:

- default route is set to cell gateway
- if cell is not online, the wifi interface will be the default route.

Examples:

1. Wifi has priority :
   cmd device cell F5521E
   cmd device wifi AR9271
   cmd device priority wifi
   cmd wlanenable 1
1. Cell has priority :
   cmd device cell F5521E
   cmd device wifi AR9271
   cmd device priority cell
   cmd wlanenable 1

See also: [Cellular], [Wi-Fi Networks]

Firmware revision 2.0.4.2360

device wifi *type*

Configure the wifi device type installed in the CTM.

type = NONE	No wi-fi device (**Default**)
type = AR9271	AR9271 USB stick
type = SR71	Ubiquiti SR71 USB stick

Examples:

1. Use SR71 wifi device as wifi client :
   cmd device wifi SR71
   cmd wlan enable 1
1. Use AR9271 wifi device as wifi access point :
   cmd device wifi SR71
   cmd wlan enable 2

See also: [Wi-Fi Networks]

Firmware revision 2.0.1.2225

dir *ppppppppp [qqqqqqqqq]*

This command sets the NAM (Number Assignment Module) value for the modem. It is a 10-digit phone number assigned to the modem by the service provider. Use the spc command to unlock the modem first. The NAM value may be queried by using the dir command without parameters. This command also sets the MIN (Mobile Identification Number) value for the modem. It is a 10-digit number assigned to the modem by the service provider. Use the spc command to unlock the modem first.

ppppppppp	10-digit phone number (NAM/MDN) to be assigned to the modem or ?+? if only MIN is to be assigned
qqqqqqqqq	10-digit phone number (MIN) to be assigned to the modem

---

Examples:

1. Set the modem?s MDN and MIN :
   cmd dir 1234567890 0987654321
1. Set the modem?s 10-digit number (NAM/MDN) :
   cmd dir 5551234567
1. Set the modem?s 10-digit number (MIN) :
   cmd dir + 0987654321
1. Query the modem?s currently assigned phone number (MDN)
   cmd dir

See also: [Cellular]

Firmware revision 1.2.0_RC3 (1133)

dmz *ip*

This command is used to set up the demilitarized zone (DMZ) feature of the modem that will let all packets go through the modem's firewall to a selected computer.

ip = 0.0.0.0	Disables the DMZ feature (**Default**)
ip = 0.0.0.x to 255.255.255.255	Local IP address to forward packets

Notes:

- If any of the modem's remote configuration features are enabled, [rmttelnet], [rmtssh], or [rmtweb], the DMZ feature will forward the enabled remote access (Telnet, SSH, or HTTP) traffic to the modem and forward all other traffic to the DMZ device.
- Port forwarding rules ([firewall]) are honored first and if no match is found then traffic is forwarded to the DMZ device.

Examples:

1. Set up all traffic to be forwarded to a device at 192.168.1.20 including remote Telnet (TCP port 23) traffic, remote SSH (TCP port 22) traffic, and remote Web configuration (TCP port 80) traffic :
   cmd dmz 192.168.1.20
1. Disable the DMZ feature :
   cmd dmz 0.0.0.0
1. Set up all traffic to be forwarded to a device at 192.168.1.20, except remote Web configuration (TCP port 80) traffic and remote SSH (TCP port 22) traffic that are forwarded to the modem :
   cmd rmtweb 1
   cmd rmtssh 1
   cmd dmz 192.168.1.20

Firmware revision 1.3.0.1586

dnscheck *n*

This command is used to enable or disable the CTM gateway from checking for valid DNS IP addresses obtained from the carrier when it connects to the network. If the DNS IP addresses are invalid, the gateway will disconnect the current network connection and reconnect.

n = 0	Disable checking for valid DNS IP addresses from the carrier
n = 1	Enable checking for valid DNS IP addresses from the carrier (**Default**)

Notes:

- After 5 reconnects have been attempted every 30 secs, and the gateway still gets an invalid DNS, the gateway will stop disconnecting and reconnecting the network connection.

Examples:

1. Disable checking DNS IP addresses from the carrier :
   cmd dnscheck 0

Firmware revision 1.3.x.1816

dout *n x [d]*

This command is used to set the state of each of the outputs. There are four outputs in total for CTM200r1 and six outputs for CTM200r2.

n = 1 to 4	Output channel number (1 to 6 for CTM200r2)
x = 0	Sets output to off (**Default**)
x = 1	Sets output to on
d = 0	Continuous duration (**Default**)
d = 1 to 255	Duration in 10ms intervals, after which output will be inverted

Notes:

- When **cmd dout** is used with **cmd save**, **d** is always **0** and the final output state is saved. The **d** duration parameter is used only for real-time purposes such as in a script (e.g. relay unlock).

Examples:

1. Set output #2 ON :
   cmd dout 2 1
1. Set output #1 ON for 2 seconds and then set it OFF :
   cmd dout 1 1 200

See also: [General Purpose IO]

Firmware revision 1.3.0 (1621)

dyndns *user password domain*

Configure the CTM gateway device to perform regular updates to the Dynamic Domain Name Service.
This feature creates an alias from a dynamic IP address to a static hostname allowing the CTM to be more easily accessed over the Internet for remote configuration or for end application.

user	Username for the DYNDNS service.
password	Password for the DYNDNS service.
domain	Domain (hostname) name for the DYNDNS

Notes:

- By default this feature is disabled.
- For this feature to work, the CTM requires a **public IP address**.
- DYNDNS updates can be disabled by setting **cmd dyndns 0 0 0.0.0.0**
- After disabling DYNDNS updates, the hostname will continue to point to the last IP address of the modem. For instructions on clearing the IP address associated with the hostname, please refer to DYNDNS documentation for details on using the offline hostname feature.

Examples:

1. Set the *user name*, *password* and the *domain name* :
   cmd dyndns cypressdemo cypress cypresscamera2.dyndns.org
1. Disable DYNDNS updates :
   cmd dyndns 0 0 0.0.0.0

Firmware revision 1.2.1 (1424)

emailsrv *ip*

This command is used to set the IP address of the SMTP email server that will be used by the modem for sending email reports.

ip = 0.0.0.0	Disabled (**Default**)
ip = 0.0.0.x to 255.255.255.255	IP address of the email server to be used for email reports

Examples:

1. Set the email server IP address to 100.120.10.10 :
   cmd emailsrv 100.120.10.10

See also: [GPS Reports], Reports?, [General Reports]

Firmware revision 1.3.0.1955

enghours *n*

Query and set the total engine hours. When a modem is installed in a vehicle and the current vehicle engine hours are known, the current engine hours will need to be programmed.

n = 0 to 999999.99	Total engine hours

Notes:

- The modem must be configured to enable engine hours counting using the [enghrmode] command.

Examples:

1. Set the engine hours to 250 :
   cmd ctm15x
   cmd enghours 250
1. Query the engine hours :
   cmd enghours

See also: [Engine Diagnostics Support]

Firmware revision 1.2.0_RC7 (rev 1187)

enghrmode *n*

Method of obtaining engine hours.

n = 0	Disabled (**Default**). Engine hours can still be obtained if vehicle has J1939 capability
n = 1	Use ignition input only (IGN ON)
n = 2	Use OBD2 input only (RPM valid and >0)
n = 3	Use combination of ignition and OBD2 inputs (RPM valid and >0 or RPM invalid and IGN ON)

Examples:

1. Use OBD2 input to obtain engine hours :
   cmd enghrmode 2

See also: [Engine Diagnostics Support]

Firmware revision 1.2.0_RC7 (rev 1187)

esn

This command queries the serial number of the embedded wireless network access device.

Notes:

- The ESN/IMEI is read only and cannot be altered.
- For CDMA/EV-DO wireless devices, this number is the 11-digit decimal ESN (Electronic Serial Number)
- For GSM/GPRS/HSPA wireless devices, this number is the 15-digit decimal IMEI (International Mobile Equipment Identity) number
- This command is not supported by all wireless network cards and modules
- When a wifi network card is used, a pseudo-ESN is calculated from the modem's Ethernet MAC

Examples:

1. Query ESN :
   cmd esn

See also: [Cellular], [universal]

ethernet *n*

This command is used to enable or disable the Ethernet services of the modem.

n = 0	Disable Ethernet services. Traffic from LAN0/LAN1 devices will not be forwarded
n = 1	Enable Ethernet services. Traffic from LAN0/LAN1 devices will be forwarded (**Default**)

Notes:

- **cmd ethernet 0** will still allow Ethernet traffic to the modem, but not through the modem to other interfaces (ie. cell, wifi).

Examples:

1. Disable Ethernet services :
   cmd ctm15x
   cmd ethernet 0

See also: [LAN]

Firmware revision 1.1.31_RC3

event add *event_description [log-level]*

Manually add an event to the event log. Added events can be reported as well.

event_description	Event description
log-level	Log-level to be written to event log (**Default 1**)

Notes:

- Added events remain in event log after power cycling the unit
- This command is not shown in **cmd event show** or **cmd showconfig**
- Spaces cannot be used in description

Examples:

1. Add "Cypress_Test" to the event log, then view the event log :
   cmd event add Cypress_Test
   cmd event dump
1. Configure event reporting on log-level 5. Add "New_Configuration" to the event log and send the event report :
   cmd event loglevel 5 5
   cmd event report 1
   cmd event add New_Configuration 5

See also: [Diagnostics and Logging]

Firmware revision 2.0.5.3052

event dump *[-f N | -h N] [-l N | -t N] [-raw] [EVENT_FILTER] [email@address]*

displays the event log with Unix timestamps converted to human readable date strings.

-f N or -h N	Dump first (head) N lines from the event log
-l N or -t N	Dump last (tail) N lines from the event log
-raw	Dump file in raw format, no conversion of Unix timestamps
EVENT_FILTER = [SEARCH_STRING]	Up to 4 event filters can be defined, eg. [PWR_CYCLE]. Only events that match the filter(s) will be displayed. This can also be applied to events within the -f / -l range.
email@address	Email the event log. SMTP server must be configured using [emailsrv], the event log will be emailed to the specified recipient.

Notes:

- the time stored in the event log can be changed via the device embedded web page Config -> TimeZone Page
- The event dump file is stored in non-volatile memory space within the CTM-200 file system (**/etc/ctm_event_log**)

Examples:

1. Dump the last 100 lines of the event log :
   cmd event dump -l 100
1. Dump the entire content of the event log :
   cmd event dump
1. Dump contents containing USB_RESET or PWR_CYCLE :
   cmd event dump [USB] [PWR]

See also: [Diagnostics and Logging]

Firmware revision 2.0.4.2480

event healthinterval *n*

Define the interval (seconds) between HEALTH status reports.

n = 600 to 86400	Number of seconds between reports (**Default 14400** or 4 hours)

Examples:

1. Define a health report to be sent every 8 hours :
   cmd event healthinterval 28800

See also: [Diagnostics and Logging]

Firmware revision 2.0.4.2480

event logclear

Clears the event log file.

Examples:

1. Clear event log :
   cmd event logclear

See also: [Diagnostics and Logging]

Firmware revision 2.0.4.2480

event dump [-f or -h N] [-l or -t N] [-raw] [EVENT_FILTER] [email@address]

displays the event log with Unix timestamps converted to human readable date strings.

-f to -h	dump first (head) N lines from the event log
-l to -t	dump last (tail) N lines from the event log
-raw	dump file in raw format, no conversion of Unix timestamps
[EVENT_FILTER]	Up to 4 event filters can be defined, eg. [PWR_CYCLE]. Only events that match the filter(s) will be displayed. This can also be applied to events within the -f / -l range.
[email@address]	email the event log. SMTP server must be configured using [cmd emailsrv], the event log will be emailed to the specified recipient.

Notes:

- the time stored in the event log can be changed via the device embedded web page Config -> TimeZone Page
- The event dump file is stored in non-volatile memory space within the CTM-200 file system

```
/etc/ctm_event_log
```

Examples:

1. Dump the last 100 lines of the event log:

```
cmd event dump -l 100
```

1. Dump the entire content of the event log:

```
cmd event dump
```

Example output:

```
Fri Sep 30 04:06:22 UTC 2011 [53]:POWER_UP
Fri Sep 30 04:06:27 UTC 2011 [58]:IGN_ON
Fri Sep 30 04:07:19 UTC 2011 [114]:CELL_ONLINE after 1 mins 1 secs offline
Fri Sep 30 05:05:24 UTC 2011 [3600]:HEALTH
Fri Sep 30 06:05:39 UTC 2011 [7200]:HEALTH
Fri Sep 30 07:05:39 UTC 2011 [10800]:HEALTH
Fri Sep 30 08:05:40 UTC 2011 [14400]:HEALTH
Fri Sep 30 09:05:40 UTC 2011 [18000]:HEALTH
Fri Sep 30 10:05:41 UTC 2011 [21600]:HEALTH
Fri Sep 30 11:05:42 UTC 2011 [25200]:HEALTH
Fri Sep 30 12:05:40 UTC 2011 [28800]:HEALTH
Fri Sep 30 13:05:44 UTC 2011 [32400]:HEALTH
Fri Sep 30 14:05:44 UTC 2011 [36000]:HEALTH
```

This command was added to the firmware in revision R2.0.4-2480

event loglevel *min max*

Set the event reporting level, events within the specified min/max range will be reported using [event report].

min = 1 to 10	Min reporting level for events (**Default 1**)
max = 1 to 10	Max reporting level for events (**Default 1**)

CTM-200 Firmware Events

CTM-200 Events	**Log Level**	**Description**
CELL_OFFLINE	10	cell is offline
CELL_ONLINE	1	cell is online (registration + IP address)
CONFIG_DROPPED	3	a config was dropped
CONFIG_RECOVERED	3	recovered from corrupt config
CONFIG_REJECTED	3	a dropped config was rejected
CONFUPGRADE	1	a cmd confupgrade has been executed
CMD_DATA_RESET	4	link data count was reset
CMD_ETHERNET	4	cmd ethernet was executed
CMD_RFSWITCH	4	cmd rfswitch was executed
ENTER_LPM	2	device has entered low power mode
ENTER_ALLOWED_ZONE	1	georoute event
EXIT_ALLOWED_ZONE	1	georoute event
ENTER_RESTRICTED_ZONE	1	georoute event
EXIT_RESTRICTED_ZONE	1	georoute event
ENGHRS_RESET	4	enghours was reset
IGN_OFF	8	ignition off
IGN_ON	8	ignition on
ODO_RESET	4	odometer was reset
POWER_UP	5	device power up
PWR_CYCLE:desc	1	cmd pwrmode 2 executed from firmware
RF_ENABLE	2	RF switch box has been turned OFF
RF_DISABLE	2	RF switch box has been turned ON
SMS_CMD	3	cmd received by SMS
SIM_PUK	2	SIM invalid PIN
USB_RESET	10	usb hard reset
VUE_CMD	3	cmd received by VUE client
WIFI_AP_UP	2	wifi AP ready
WIFI_OFFLINE	2	wifi client online
WIFI_ONLINE	2	wifi client offline
UPGRADEFW	1	a cmd upgradefw has been executed
CMD_DATA_RESET:OK|FAIL	4	cmd data 0
FUEL_RESET:OK|FAIL	4	cmd fuel reset
SET_FUEL:<value> OK|FAIL	4	cmd fuel query <value>

SET_FUEL_RATE:<resetbyign> <deltadistance> <deltatime> OK|FAIL	4	cmd fuel rate <resetbyign> <deltadistance> <deltatime>
ENGHRS_RESET:<value> OK|FAIL	4	cmd enghours <value>
CMD_ETHERNET:0|1	4	cmd ethernet 0|1
SET_IDLE:<value> OK|FAIL	4	cmd idle query <value>
RESET_IDLE:OK|FAIL	4	cmd idle reset
ODO_RESET:<value> OK|FAIL	4	cmd odometer reset <value>
CMD_RFSWITCH:0|1	4	cmd rfswitch 0|1

Examples:

1. Set the loglevel range between 1 and 5 :
   cmd event loglevel 1 5

See also: [Diagnostics and Logging]

Firmware revision 2.0.4.2480

event minoffline *n*

Sets the minimum time interval (seconds) before reporting a CELL_ONLINE event. By increasing the time for this command, CELL_ONLINE events will only be generated by continuous connectivity.

n	Number of seconds (**Default 120**)

Examples:

1. Define a minimum time of 300 (5 minutes) before a CELL_ONLINE event is generated :
   cmd event minoffline 300

See also: [Diagnostics and Logging]

Firmware revision 2.0.4.2480

eventreport *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

Report event log events.

r1 to r8 = 0	Disables the report (**Default**)
r1 to r8 = 1 to 999	General report to use for event reports
r1 to r8 = 1020 to 1027	**(Firmware 3034 and above)** GPS reports 1 to 8
r1 to r8 = 1040 to 1047	**(Firmware 3034 and above)** I/O reports 1 to 8

Examples:

1. Report events using general reports 1 and 2 :
   cmd event report 1 2
2. Report events using IO report #6 (*1045*) :
   cmd event report 1045

See also: [Diagnostics and Logging], [General Reports]

Firmware revision 2.0.4.2480

firewall *n extport locport t ip s*

This command is used to setup the port forwarding configuration of the modem.

n = 1 to 50	Port forwarding number
extport = 0 to 65535	External port number to forward to
locport = 0 to 65535	Local port number to forward to
t = 0	Disable
t = 1	UDP
t = 2	TCP
t = 3	Both UDP and TCP
ip = 0.0.0.0 to 255.255.255.255	Local IP address to forward to
s = 0	Disable forwarding
s = 1	Enable forwarding

Notes:

- Up to 50 port forwarding configurations can be set.
- The local IP address will default to 192.168.1.X, where X is extracted from iii.iii.iii.iii and 192.168.1 is extracted from the IP address in the LAN Configuration setting.
- LAN IP addresses used in port forwarding rules must match the LAN subnet as configured using [lanip], [lannetmask], and [lanrepip].
- The corresponding Port Forwarding Rules (PortFwd) page in the Web Interface only shows the first 10 port forwarding configurations.

Examples:

1. Set port forwarding #1 to forward data destined for port 8080 (same external & local port number), for both UDP and TCP, to IP 192.168.1.20 and enabled :
   cmd firewall 1 8080 8080 3 192.168.1.20 1
1. Set port forwarding #2 to forward UDP data destined for external port 42375 and redirect it to local port 5001 at IP 192.168.1.20 and enabled :
   cmd firewall 2 42375 5001 1 192.168.1.20 1

See also: [Friends List]

freeconsole

Kill the serial console shell process. This command must be done at first if you use [gopad] or [modbusgw] from the SSH/Telnet console in [mode 4] or [mode 6].

Notes:

- The serial console is not available after this command. You may need to set [port] to use serial console again.

Examples:

1. Free the serial console port for use by pad or modbusgw mode :
   cmd freeconsole
   cmd gopad
   cmd modbusgw

See also: [Serial Port Settings]

friends *n ip netmask [t]*

This command is used to setup the modem's firewall friends list, which is used to block incoming packets from an IP address that is not specifically enabled.
Use this to define a range of IP addresses whose traffic you wish to be accepted by the modem.

n = 1 to 8	Friends list number
ip = 0.0.0.0 to 255.255.255.255	IP address/range to allow
netmask = 0.0.0.0 to 255.255.255.255	Netmask of addresses to allow
t = 0	Control access to INPUT
t = 1	Control access to FORWARDING
t = 2	Control access to both INPUT and FORWARDING

Notes:

INPUT controls access to the following modem features:

- MODBUS
- PAD
- ULCP
- Remote SSH access
- Remote Telnet access
- Remote Web access

FORWARDING controls access to:

- Port forwarding configured via [firewall]
- DMZ feature configured via [dmz]

- Modem access is verified in ascending order via the OR condition of all entries in the friends list.
- By default, the friends list is disabled and all IP addresses are allowed to access the modem.

Examples:

1. Allow only incoming requests from the IP address 1.2.3.4 to access the modem :
   cmd friends 1 1.2.3.4 255.255.255.255
1. Allow only incoming requests from the 1.2.3.x subnet to access the modem :
   cmd friends 2 1.2.3.0 255.255.255.0
1. Disable the friends list entry and allow all IP addresses to access the modem (default) :
   cmd friends 1 0.0.0.0 0.0.0.0

See also: [DMZ], [Port Forwarding]

Firmware revision 2.0.4.2658

ftp remote *n*

Enable/disable remote ftp access to the CTM.

n = 0	Disable remote ftp (**Default**)
n = 1	Enable remote ftp

Examples:

1. Enable remote ftp access to the CTM :
   cmd ftp remote 1

See also: [FTP]

Firmware revision 2.0.5.2995

ftp server *n*

Enable/disable the CTM FTP server.

n = 0	Disable ftp server (**Default**)
n = 1	Enable ftp server

Notes:

- Pure-ftpd is the CTM-200 ftp server package.
- The pure-ftpd bandwidth options have been set to 100KB/s.

Examples:

1. Enable FTP service :
   cmd ftp server 1

See also: [FTP]

Firmware revision 2.0.3.2289

fuel io *n x y z*

Configures the total fuel calculation to use GPIO inputs.

n = 1 to 6	GPIO used (**Default 1**)
x = 0 to 10	GPIO reading at empty (current or voltage) (**Default 0**)
y = 0 to 10	GPIO reading at full (current or voltage) (**Default 10**)
z = 1 to 65535	Number of liters required to reach full (**Default 100**)

Notes:

- **cmd fuel mode 5** must be set

Examples:

1. Use input 1, 0V input when empty, 10V when full and a full tank taking 100 Liters :
   cmd fuel io 1 0 10 100

See also: [Fuel Rate]

Firmware revision 2.0.4.2591

fuel mode *n*

Set the fuel calcuation method.

n = 0	Disables fuel calculation (**Default**)
n = 1	Use OBDII MAF (mass air flow rate) parameters for FUEL calculation (this setting requires an interface with the vehicle ECU) (p13)
n = 2	Use J1939 total fuel parameter (p31)
n = 3	Use J1939 fuel rate parameter (p34)
n = 4	Use J1939 average fuel parameter (p41)
n = 5	Use GPIO connected to analog fuel gauge for total fuel calculation

---

Examples:

1. Configure the fuel to be calculated using data from the vehicle Engine control unit (ECU) (via OBDII) :
   cmd fuel mode 1

See also: [Fuel Rate], [Vehicle Support], [OBD2/J1939 Parameters Table]

Firmware revision 2.0.4.2591

fuel query

Query the total fuel used (liters) in a vehicle with fuel calculation enabled.

Examples:

1. Query the fuel value :
   cmd fuel query

See also: [Fuel Rate]

Firmware revision 2.0.4.2623

fuel rate *i d t*

Sets whether timer or distance or both triggers when fuel rate is calculated. Whenever d or t triggers a calculation, both triggers are reset.

i = 0	Disable ignition based reset (**Default**)
i = 1	Enable ignition based reset
d = 0 to 65535	Delta distance in km to trigger fuel rate calculation (**Default 1**)
t = 0 to 65535	Delta time in seconds to trigger fuel rate calculation (**Default 60**)

Notes:

- Fuel rate is calculated by taking the difference between two total fuel readings obtained at different times based on an incrementing odometer "delta" value and factoring it to a L/100Km value.
- Fuel rate calculation requires active data from a connected OBDII/J1939/GPS/GPIO interface and [fuel mode] to be configured.

Examples:

1. Configure the fuel rate to be calculated based on a "delta" odometer value of 25 km :
   cmd fuel rate 0 25 0
1. Configure the fuel rate to be calculated every minute :
   cmd fuel rate 0 0 60
1. Configure the fuel rate to be reset after each ignition ON and calculate fuel rate after every 60 seconds :
   cmd fuel rate 1 0 60
1. Configure the fuel rate to be reset after each IGN ON and to calculate fuel rate every 60s or every 100km, whichever is reached first :
   cmd fuel rate 1 100 60

See also: [Fuel Rate]

Firmware revision 2.0.4.2690

fuel rate query

Query the fuel rate value.

Notes:

- This command will return ERROR if the minimum distance set by [fuel rate] has not been met or if no fuel or odometer data is available.
- Fuel rate calculation requires active data from a connected OBDII/J1939/GPS/GPIO interface and [fuel mode] to be configured.

Example:

1. Query fuel rate :
   cmd fuel rate query

See also: [Fuel Rate]

Firmware revision 2.0.4.2655

fuel rate reset

Resets the fuel rate value to 0.

Examples:

1. Resets the fuel rate :
   cmd fuel rate reset

See also: [Fuel Rate]

Firmware revision 2.0.4.2690

fuel reset

Resets the fuel value to 0.

Examples:

1. Reset the fuel value.
   cmd ctm15x
   cmd fuel reset

See also: [Fuel Rate]

Firmware revision 2.0.4.2690

geort acount

View Geo-Route's exited allowed area alarm (`$PGRT ALRMA messages`) counter. This value is non-volatile.

Examples:

1. View the number of times exited allowed area alarm was triggered :
   cmd geort acount
1. Reset the counter to 0 :
   cmd geort acount 0

See also: [Geo-Routing]

Firmware revision 2.0.4.2607

geort c2bin *[-d]*

Convert text-based route list stored in `/etc/geort/rt` into a CTM binary format. '-d' flag will display the result after conversion. Warning: If the route is long, it may take a while to display all the values.

Notes:

- This command is not required when the route file is uploaded via [geort update] as the conversion process is built into the update command
- Files must be stored in /etc/geort/rt
- Filenames must be geolsN.txt (N=1 to 32) (e.g. geols1.txt, geols32.txt)
- File content must be of the following format:

```
[radius (m)] [longitude 1] [latitude 1] [longitude 2] [latitude 2] [zone (allowed:1|restricted:2)]
```

Example:

```
500 -122.991268 49.254447 -122.983114 49.245875 1
300 -122.983114 49.245875 -123.019163 49.258341 1
500 -123.019163 49.258341 -123.058302 49.250161 1
```

- Each file can only contain 1 zone type

Examples:

1. To convert the files :
   cmd geort c2bin
1. To convert the files and view the result :
   cmd geort c2bin -d

See also: [Geo-Routing]

Firmware revision 2.0.4.2607

geort delete *route*

Deletes Geo-Routes from active routes.

route = ALL	Delete ALL routes
route = 1 to 32	Geo-Route to delete

Examples:

1. To disable all routes :
   cmd geort delete all
1. To disable route 3 :
   cmd geort delete 3

See also: [Geo-Routing]

Firmware revision 2.0.4.2639

geort enable *n*

Disable or enable Geo-Route.

n = 0	Geo-Route disabled (**Default**)
n = 1	Geo-Route enabled

Examples:

1. To enable Geo-Route :
   cmd geort enable 1

See also: [Geo-Routing]

Firmware revision 2.0.4.2607

geort list *[n | -w]*

Display Geo-Routes being monitored.

n = 1 to 32	View midpoints for route n
-w	Print list in wide format

Examples:

To print entire list :
cmd geort list

```
1 1
2 1
3 1
4 0
5 0
6 0
7 0
8 0
9 0
10 0
11 0
12 0
13 0
14 0
15 0
16 0
17 0
18 0
19 0
20 0
21 0
22 0
23 0
24 0
25 0
26 0
27 0
28 0
29 1
30 0
31 0
32 1
```

To print list in wide format :
cmd geort list -w

```
1, 2, 3, 10, 11, 32
OK
```

To print the midpoints of a specific route :
cmd geort list 3

```
0 RSq:0.640000 LnFSq:5273.190918 Lon:-123.017014 Lat:49.282925 st:2
1 RSq:0.124916 LnFSq:5276.592285 Lon:-122.969635 Lat:49.267021 st:2
2 RSq:0.124916 LnFSq:5276.589355 Lon:-122.970993 Lat:49.267036 st:2
3 RSq:0.124916 LnFSq:5276.586914 Lon:-122.972343 Lat:49.267048 st:2
4 RSq:0.124916 LnFSq:5276.583984 Lon:-122.973694 Lat:49.267063 st:2
```

```
5 RSq:0.124916 LnFSq:5276.581055 Lon:-122.975052 Lat:49.267075 st:2
6 RSq:0.124916 LnFSq:5276.578125 Lon:-122.976402 Lat:49.267090 st:2
7 RSq:0.124916 LnFSq:5276.575684 Lon:-122.977760 Lat:49.267101 st:2
8 RSq:0.124916 LnFSq:5276.572754 Lon:-122.979111 Lat:49.267117 st:2
9 RSq:0.124916 LnFSq:5276.569824 Lon:-122.980461 Lat:49.267128 st:2
10 RSq:0.124916 LnFSq:5276.566895 Lon:-122.981819 Lat:49.267143 st:2
11 RSq:0.124916 LnFSq:5276.563965 Lon:-122.983170 Lat:49.267155 st:2
12 RSq:0.124916 LnFSq:5276.561523 Lon:-122.984520 Lat:49.267166 st:2
13 RSq:0.124916 LnFSq:5276.558594 Lon:-122.985878 Lat:49.267181 st:2
14 RSq:0.124916 LnFSq:5276.555664 Lon:-122.987228 Lat:49.267193 st:2
15 RSq:0.124916 LnFSq:5276.552734 Lon:-122.988579 Lat:49.267208 st:2
16 RSq:0.124916 LnFSq:5276.550293 Lon:-122.989937 Lat:49.267220 st:2
17 RSq:0.124916 LnFSq:5276.547363 Lon:-122.991287 Lat:49.267235 st:2
18 RSq:0.124916 LnFSq:5276.544434 Lon:-122.992638 Lat:49.267246 st:2
19 RSq:0.160000 LnFSq:5276.784180 Lon:-123.013237 Lat:49.266125 st:2
OK
```

See also: [Geo-Routing]

Firmware revision 2.0.4.2607

geort period *m*

Set how often Geo-Route violation is checked.

m = 10 to 300	Seconds to wait between each Geo-Route check (**Default 60**)

Examples:

1. To set Geo-Route to be checked every 10 seconds :
   cmd geort period 10

See also: [Geo-Routing]

Firmware revision 2.0.4.2607

geort rcount

View Geo-Route's restricted area alarm (`$PGRT ALRMR messages`) counter. This value is non-volatile.

Examples:

1. View the number of times restricted area alarm was triggered :
   cmd geort rcount
1. Reset the counter to 0 :
   cmd geort rcount 0

See also: [Geo-Routing]

Firmeware revision 2.0.4.2607

geort report *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

Associate up to 8 reports for Geo-Route.

r1 to r8 = 0 to 999	Report number

Notes:

- **cmd geort report 0** will delete all reports.
- Each report will be composed of the following message:
  $PGRT,ddmmyy,hhmmss.ss,v,MSG,rr,LAT,LON,hhh.h,sss.s,MODEMID*hh
  where
  v is validity flag (A = valid, V = invalid)
  MSG can be:

    "ALRMA" - alarm when allowed area violation counter has reached set threshold
    "ALRMR" - alarm when restricted area violation counter has reached set threshold
    "AOUT" - when vehicle has exited an allowed area
    "AIN" - when vehicle has entered an allowed area
    "ROUT" - when vehicle has exited a restricted area
    "RIN" - when vehicle has entered a restricted area

  rr is route number
  LAT/LON is the GPS location in decimal degrees (ddd.dddd)
  hhh.h is heading
  sss.s is speed
  MODEMID is modem ID (ESN/IMEI)
  hh is NMEA checksum

  Example messages:

```
$PGRT,101111,173834.00,A,AIN,1,49.253613,-122.997253,000.6,153.0,354155040009270*2A
$PGRT,101111,173514.00,A,AOUT,0,49.253792,-122.997681,000.5,150.0,354155040009270*6E
$PGRT,101111,173514.00,A,RIN,1,49.253792,-122.997681,000.5,150.0,354155040009270*35
$PGRT,101111,173834.00,A,ROUT,0,49.253613,-122.997253,000.6,153.0,354155040009270*71
$PGRT,101111,173554.00,A,ALRMR,1,49.253765,-122.997597,000.5,148.0,354155040009270*21
$PGRT,101111,173634.00,A,ALRMA,0,49.253696,-122.997513,000.4,133.0,354155040009270*3A
```

Examples:

1. To set Geo-Route to be checked every 10 seconds and reporting to reports 1, 2 and 999:
   cmd geort period 10
   cmd geort report 1 2 999

See also: [Geo-Routing], [General Reports]

Firmware revision 2.0.4.2607

geort th *r t*

Set the number of consecutive violations encountered before a corresponding alarm (ALRMA/ALRMR) message is generated. The counter is reset when an alarm is sent. Note that AIN/AOUT and RIN/ROUT do not have thresholds - they are always sent when they occur.

r = 1 or 2	Zone type (1-Allowed zones, 2-Restricted zones)
t = 1 to 255	Threshold (number of violations before $PGRT ALRMA/ALRMR message is sent)

Notes:

Default:

- cmd geort th 1 5
- cmd geort th 2 3

Example messages:

```
$PGRT,101111,173554.00,A,ALRMR,1,49.253765,-122.997597,000.5,148.0,354155040009270*21
$PGRT,101111,173634.00,A,ALRMA,0,49.253696,-122.997513,000.4,133.0,354155040009270*3A
```

Examples:

1. To set Geo-Route to send an alarm after the vehicle is outside of all allowed zones for 3 times (checks) in a row :
   cmd geort th 1 3
1. To set Geo-Route to send an alarm after the vehicle is in a restricted zone for 2 times (checks) in a row :
   cmd geort th 2 2

See also: [Geo-Routing]

Firmware revision 2.0.4.2607

geort update *r u [n] [p]*

Add/update Geo-Routes from specified location.

Please note that previous routes with identical route number will be deleted if routes are successfully updated!

r = 1 to 32	Update specific Geo-Route
r = all	Update all Geo-Routes
u = localhost	Localhost, image must be in /tmp
u = url	URL, can be IP address. Prefixed by ftp:// or http://, if no prefix is specified (eg. cypress.bc.ca) then ftp:// is used.
n = username	Username for server (Optional)
p = password	Password for server (Optional)

Notes:

- When **localhost** is specified, Geo-Route files must be located in **/tmp** on the CTM. However, when **?localhost://t2** is specified, files must be located in **/t2** on the CTM.

Examples:

Download all Geo-Routes from remote server via ftp :
cmd geort update all 192.168.1.20 kmo kmotest

```
Downloading Geo-Routes...
Verifying download...
Copying files...
Converting Geo-Routes...
Cleaning up...
Done!
```

1. Download a specific Geo-Route (route 5) from /grt directory via ftp :
   cmd geort update 5 ?ftp://192.168.1.20/grt kmo kmotest
1. Download a specific Geo-Route (route 1) locally (located in /tmp) :
   cmd geort update 1 localhost
1. Download a specific Geo-Route (route 2) locally (located in /tmp/t2) :
   cmd geort update 2 ?localhost://tmp/t2
1. Download all Geo-Routes locally (located in /t2) :
   cmd geort update ALL ?localhost://t2

See also: [Geo-Routing]

Firmware revision 2.0.4.2639

gopad *n*

Manually initiates a PAD connection on the CTM's serial port(s).

n = 1	First PAD configuration (Serial Port 1,2,3) (**Default 1**)
n = 2	Second PAD configuration (Serial Port 2,3)

Notes:

- [freeconsole] must be run first before using this command
- [mode] must be configured as one of **4, 17, 18, 19** for this command to initiate a PAD connection

---

Examples:

1. Initiate PAD manually :
   cmd freeconsole
   cmd gopad

See also: [PAD]

Firmware revision 1.3.0.2069

gpsaccel *n a [d]*

Sets the GPS report triggers using GPS based hard acceleration and deceleration events.
Reports will be triggered if the instantaneous acceleration is greater than **a** or the instantaneous acceleration is less than **d**.

n = 1 to 8	GPS report number
a >= 0	Acceleration threshold in km/h/s (**Default 0**)
d <= 0	Deceleration threshold in km/h/s (**Default 0**)

Examples:

1. Send GPS report #7 whenever acceleration is greater than 10 km/h/s or deceleration is less than -15 km/h/s :
   cmd gpsaccel 7 10 -15

See also: [GPS Configuration], [GPS Reports]

Firmware revision 1.1.31

gpsaddmes *n m1 [m2] [m3] [m4]*

Adds messages to a GPS report.

n = 1 to 8	GPS report number
m1 to m4	Message type to be added, valid message types must be used [See message list]

Notes:

- Binary messages MUST be placed before ASCII messages. Ex. **cmd gpsaddmes 1 85 114** = correct, **cmd gpsaddmes 1 114 85** = incorrect.
- 4 messages can be included in a single report. Duplicate messages cannot be included in a report.
- Messages will be sent in a report in the same order that they are added with this command.
- ULCP header messages will be sent as individual UDP packets, NMEA format messages will be combined into a single packet.

Examples:

1. Adds message #16 ? GPS NMEA GLL ? to GPS report #4 :
   cmd gpsaddmes 4 16

See also: [GPS Reports]

gpscond *n b t [d] [ms Ms] [h hs] [mt]*

Sets the condition(s) that will trigger a GPS report.
The conditional operator is used to indicate how all following parameters will be used to determine if a report is triggered.

n = 1 to 8	GPS report number
b = 0	Conditional operator for all following parameters: **Off** (**Default**)
b = 1	Conditional operator for all following parameters: **AND**
b = 2	Conditional operator for all following parameters: **OR**
t = 0	Timeout disabled (**Default**)
t = 1 to 65535	Timeout in seconds
d = 0 to 65535	Distance traveled threshold in meters (**Default 0**)
ms = 0 to 65535	Low speed threshold in kph ? use with Ms (**Default 0**)
Ms = 0 to 65535	High speed threshold in kph ? use with ms (**Default 0**)
h = 0 to 359	Heading change in degrees ? use with hs (**Default 0**)
hs = 0 65535	Minimum speed threshold to make heading measurement valid, in kph. Use with **h** (**Default 0**)
mt = 0 to 65535	Maximum reporting rate in seconds (minimum time between reports) (**Default 0**)

Notes:

- The **mt** parameter must be used at the end if all other optional parameters are entered.

Examples:

1. Send report #1 every **60** seconds :
   cmd gpscond 1 1 60
1. Send report #2 every **60** seconds **AND** when distance traveled is greater than **50** metres :
   cmd gpscond 2 1 60 50
1. Send report #4 every **60** seconds **AND** when distance is greater than **50** metres **AND** the speed is between **20kph** and **60kph** :
   cmd gpscond 4 1 60 50 20 60
1. Send report #5 every **60** seconds **OR** when distance is greater than **50** metres **OR** speed is greater than **60kph**, **OR** if the heading changes by more than **45** degrees, with a maximum report rate of one every **10** seconds :
   cmd gpscond 5 2 60 50 60 200 45 10 10
1. Send report #6 only when distance traveled is greater than **0** metres **AND** the speed is between **0kph** and **5kph AND** with a maximum report rate of one every **7** seconds :
   cmd gpscond 6 1 0 0 0 5 0 0 7

See also: [GPS Configuration], [GPS Reports]

gpsdata

Displays the current status of GPS input devices configured via [gpsinput] and corresponding GPS data.

Examples:

1. Display status of currently configured GPS input devices and GPS data obtained from the devices :
   cmd gpsdata

See also: [GPS Configuration]

gpsdelmes *n m*

This command is used to delete a message type (or all messages) from a GPS report.

n = 1 to 8	GPS report number
m	Message type to be deleted (0 to delete all messages)

Examples:

1. Delete message type #16 from GPS report #1 :
   cmd gpsdelmes 1 16
1. Delete all messages from GPS report #4 :
   cmd gpsdelmes 4 0

See also: [GPS Reports]

gpsdgps *n*

Configure DGPS mode and SBAS. DGPS correction data source will be set as WAAS or RTCM.

n = 0	Disables DGPS mode and search of SBAS satellite (**Default**)
n = 1	Enables search of SBAS satellite and sets DGPS correction data source as RTCM
n = 2	Enables search of SBAS satellite and sets DGPS correction data source as WAAS

Examples:

1. Enable search of SBAS satellite and set DGPS correction data source as RTCM :
   cmd gpsdgps 1

See also: [GPS Configuration]

Firmware revision 2.0.5.2893

gpsemail *n emailaddr*

Sets the email address that the GPS report will be sent to.
Up to 8 email addresses may be configured ? one for each of the 8 GPS reports. The default email address is blank.

(leave blank to clear the address)

Notes:

- An email server is required ? see [emailsrv].

Examples:

1. Set the destination email address for GPS report #1 :
   cmd gpsemail 1 me@cypress.bc.ca
1. Clear the email address for GPS report #1 :
   cmd gpsemail 1

See also: [GPS Reports]

gpsgga

Displays the current GPS position in NMEA0183 format.
This command is a read only command.

Examples:

1. Return a current GPS NMEA format GGA message :
   cmd gpsgga

See also: [GPS Configuration]

gpsinput *m*

This command defines what source to use for GPS data.

m = 1	Use internal GPS module (TSIP) (Not available for CTM200)
m = 2	Use internal GPS module (NMEA) (Not available for CTM200)
m = 4	Use external GPS module (NMEA)
m = 8	Use A-GPS module (NMEA)
m = 16	Use internal GPS module (CTM200 only)

Notes:

- Use **cmd gpsinput m** where **m** is the sum of the **m** input values

---

Examples:

1. Use external GPS and A-GPS modules :
   cmd gpsinput 12

See also: [GPS Configuration]

gpslocip *n ipaddr*

Sets the IP address of the local server that the GPS report will be sent to.
Up to 8 GPS reports can be configured.

n = 1 to 8	GPS report number
ipaddr = 0.0.0.0 to 255.255.255.255	Local IP address in decimal (**Default 0.0.0.0**)

Notes:

- If a report has no **gpslocip** configured, then the global local IP address configured with [lanrepip] (default 192.168.1.20) will be used.
- **firmware 3396** and later can broadcast local UDP messages.

Examples:

1. Report #1 will be sent to local IP address 192.168.1.21 :
   cmd gpslocip 1 192.168.1.21
2. Report #2 will be broadcasted on the local 192.168.1.0/24 subnet (**firmware 3396 and later**) :
   cmd gpslocip 2 192.168.1.255

See also: [GPS Reports]

Firmware revision 1.3.0.1967

gpslocport *n port*

Sets the port number of the local server that the GPS report will be sent to.
Up to 8 GPS reports may be configured.

n = 1 to 8	GPS report number
port = 0 to 65535	Local port number (**Default 0**)

Examples:

1. Send report #1 to local port 5005 :
   cmd gpslocport 1 5005

See also: [GPS Reports]

gpsmes

Displays all messages associated with each GPS report.
This command is read only.

Examples:

1. Display all messages associated with each GPS report :
   cmd gpsmes

See also: [GPS Reports]

gpsparam *input priority port br db p sb fc*

This command configures the parameters and priority of the port the modem will use for obtaining GPS information.

input	GPS input to configure (1-5)
input = 1	Use internal GPS module (TSIP) **(Not available for CTM200)**
input = 2	Use internal GPS module (NMEA) **(Not available for CTM200)**
input = 3	Use external GPS module (NMEA)
input = 4	Use A-GPS module (NMEA)
input = 5	Use internal GPS module **(CTM200 only)**
priority = 0 to 3	Data Priority. 0=highest
port	Serial port to use. e.g. ttyS1 or ttyUSB14
br	baud rate (see cmd port)
db	data bits (see cmd port)
p	parity (see cmd port)
sb	stop bits (see cmd port)
fc	flow control (see cmd port)

Notes:

- If all enabled ports are available and have valid GPS, the highest priority input is used.
- This can feature can also be used for A-GPS since it is outputting NMEA data on a ttyUSB port.
- When GPS inputs are configured at the same priority, GPS data will be obtained from whichever GPS input has valid data first, in ascending order from GPS input 0 to GPS input 3.

Examples:

1. configure the modem USB port for accepting GPS data :
   cmd gpsparam 3 2 /dev/ttyUSB0 4800 8 n 1 0
1. configure the modem external serial port for accepting GPS data :
   cmd gpsparam 3 2 /dev/ttyS0 4800 8 n 1 0
1. configure a CTM200 modem to use internal GPS :
   cmd gpsparam 5 0 none

See also: [GPS Reports]

gpspos *n ±xx.xxxxxx ±yyy.yyyyyy*

Set fixed GPS position mode. This sets the GPS coordinates used in modem reports to user-defined latitude and longitude values. When this setting is enabled, the GPS date and time used in modem reports is synchronized to the modem's system time.

This setting is used for monitoring modems used with fixed-site applications.

n = 0	Disable fixed GPS position mode. Use GPS position from GPS input device configured with [gpsinput]. (Default)
n = 1	Enable fixed GPS position mode. Use user-defined location.
±xx.xxxxxx = -90.000000 <= ±xx.xxxxxx <= +90.000000	latitude in decimal format, where North=positive and South=negative
±yyy.yyyyyy = -180.000000 <= ±yyy.yyyyyy <= +180.000000	longitude in decimal format where East=positive and West=negative

A **cmd save** and a **power cycle** are required for this command to take effect.

Examples:

1. Enable fixed GPS position mode and set the user-defined location to (49.256553, -122.996733) :
   cmd gpspos 1 49.256553 -122.996733
1. Disable fixed GPS position mode but preserve the user-defined location :
   cmd gpspos 0
1. Disable fixed GPS position mode and clear the user-defined location :
   cmd gpspos 0 0 0

See also: [GPS Configuration]

Firmware Revision R1.3.0.1927

gpsremip *n iii.iii.iii.iii*

Sets the IP address of the remote server that the GPS report will be sent to. Up to 8 GPS reports can be configured.

n = 1 to 8 or 11	GPS report number
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	remote IP address in decimal

---

Examples:

1. Report #1 will be sent to remote IP address 123.10.1.101 :
   cmd gpsremip 1 123.10.1.101

See also: [GPS Reports]

gpsremport *n xxxxx*

Sets the IP port number of the remote server that the GPS report will be sent to.
Up to 8 GPS reports can be configured.

n = 1 to 8 or 11	GPS report number
xxxxx = 0 to 65535	remote port number in decimal

Examples:

1. Report #1 will be sent to port 5005 on remote IP address set by [gpsremip] :
   cmd gpsremport 1 5005

See also: [GPS Reports]

gpsrep *n l r s*

Sets the reporting type for each GPS report for the local and remote servers.

n = 1 to 8 or report 11	GPS report number
l = 0	disables local GPS report (default)
l = 1	asynchronous NMEA or ULCP messages over RS232
l = 2	asynchronous NMEA or ULCP messages with a ULCP header over RS232
l = 3	in-band NMEA or ULCP messages in a UDP Packet over Ethernet **Firmware 3211 and below**
l = 3	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets over Ethernet **Firmware 3232 and above**
l = 4	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets over Ethernet sent in binary format only
l = 5	in-band NMEA or ULCP messages in a TCP Packet over Ethernet **Firmware 3211 and below**
l = 5	in-band NMEA or ULCP messages with a ULCP header in individual TCP Packets over Ethernet **Firmware 3232 and above**
l = 6	file-based reports
r = 0	disables remote GPS report (default)
r = 3	in-band NMEA or ULCP messages in a UDP Packet **Firmware 3211 and below**
r = 3	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets **Firmware 3232 and above**
r = 4	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets in binary format only
r = 5	in-band NMEA or ULCP messages in a TCP Packet **Firmware 3211 and below**
r = 5	in-band NMEA or ULCP messages with a ULCP header in individual TCP Packets **Firmware 3232 and above**
r = 6	email reports
r = 7	SMS reports
s = 0	disables the store and forward of GPS reports
s = 1	enables the store and forward of GPS reports

Notes:

- For **r = 7** (SMS reports), the total length of the report must not exceed 166 characters including <CR> and <LF>
- A remote report cannot be configured when using **l = 6** (File-based reporting).

Examples:

1. Send GPS report #4 as a UDP packet over Ethernet and over the wireless link, do not store GPS reports :
   cmd gpsrep 4 3 3
1. Send GPS report #2 as a UDP packet over Ethernet and as an SMS message to the SMS destination set using the gpssms command, and enable the store and forward of GPS reports :
   cmd gpsrep 2 3 7 1

See also: [GPS Reports]

gpsrmc

Displays the current GPS position in NMEA0183 format.
This command is a read only command.

Examples:

1. Return a current GPS NMEA format RMC message :
   cmd gpsrmc

See also: [GPS Configuration]

gpssms *n ppppppppppp|emailaddr*

Sets the destination of the GPS report that is sent as an SMS message.

n = 1 to 8	GPS report number
ppppppppppp	phone number which the SMS report will be sent to. For long distance calls, a ?1? needs to be added In front of the phone number.
emailaddr	email address which the SMS report will be sent to.

Notes:

- SMS features are only available for specific manufacturer, RF modules, cards or devices. Please contact Cypress Solutions for a complete list of products that support SMS functionality.

Examples:

1. Send GPS report #1 as an SMS message to the specified phone number :
   cmd gpssms 1 1234567890
2. Send GPS report #2 as an SMS message to the specified email address :
   cmd gpssms 2 me@?

See also: [GPS Reports]

gpstime *n*

Set the priority of valid GPS as an external system time synchronization source.

n = 0	Disabled
n = 1-3	Priority relative to other external system time synchronization sources with 1 = highest (**default = 1**)

Examples:

1. Set valid GPS as lowest priority relative to other external time synchronization sources :
   cmd gpstime 3

See also: [Time Synchronization]

Firmware revision 1.3.0.1729

idle cond *n a b c*

Set the Idle reporting and reset condition.

n = 1 to 8	idle condition number
a = 0	idle START trigger disabled (**default**)
a = 1	idle START trigger enabled, idle event will be triggered when idle > idle time
b = 0	idle END trigger disabled, idle event triggers when vehicle leaves idle state (**default**)
b = 1	idle END trigger enabled, idle event triggers when vehicle leaves idle state
c = 0	idle time accumulates, reset is via "cmd idle reset"
c = 1	idle time is reset at **b=1**
c = 2	idle time is reset at **a=1** (state of **b** is ignored)

Examples:

cmd idle time 300 : Set idle time to 5 mins. Used in all following examples

1. Idle event will trigger twice. When idle time > 5 minutes AND when vehicle leaves idle state (ie starts moving) at which time idle will be reset :
   cmd idle cond 1 1 1 1
2. Idle event will trigger twice. When idle when idle time > 5 minutes AND when vehicle leaves idle state (ie, starts moving). Total idle time will NOT be reset :
   cmd idle cond 1 1 1 0
3. Idle event will trigger once, when idle > idle time. When vehicle leaves idle, no event is generated, cumulative idle is reset :
   cmd idle cond 1 1 0 2
4. INVALID case. Idle event will NOT trigger. Total idle time will NOT be reset :
   cmd idle cond 1 0 1 2
5. Idle event will trigger once, when vehicle leaves idle, cumulative idle is reset after event :
   cmd idle cond 1 0 1 1
6. Idle event will trigger once, when idle > idle time, cumulative idle is reset after event :
   cmd idle cond 1 1 0 1

See also: [Idle Time]

Available in firmware revision R2.0.5-2812 and later.

idle mode *n*

Set the Idle mode for vehicle idling condition.

n=0	Disables Idle calculation
n=1	Use OBDII/J1939 parameters for IDLE calculation. This setting requires an interface with the vehicle ECU.
n=2	Use GPS PVT(position, velocity, time) information along with ignition sense for idle calculation. This setting requires the ignition control line of the CTM to be wired to the vehicle ignition and valid GPS signal

---

Examples:

1. Configure the idle time to be calculated using data from the vehicle Engine control unit (ECU) (via OBDII or J1939) :
   cmd idle mode 1

See also: [Idle Time]

Available in firmware revision R2.0.4-2575 and later.

idle query

Query the Idle time (seconds) for a vehicle with idle detection enabled.

Examples:

1. Query idle time :
   cmd idle query

See also: [Idle Time]

Available in firmware revision R2.0.4-2575 and later.

idle report *n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for IDLE triggered reports.
Up to 8 IDLE triggers can be configured, each supporting up to 8 reports.

n = 1 to 8	IDLE trigger condition
r1...r8 = 1 to 999	Report number
r1...r8 = 0	Disables the report

Examples:

1. Set report #2 and #5 for IDLE trigger condition #1. **cmd idle report 1 2 5**

See also: [Idle Time]

idle reset

Resets the idle time to 0.

Examples:

1. reset idle time :
   cmd ctm15x
   cmd idle reset

See also: [Idle Time]

Firmware revision R2.0.4-2575

idle time *n*

Set the Idle time for vehicle idling condition to start being recorded.

n	Idle time in seconds

Examples:

1. Set the time at which idle detection will start to 5 minutes :
   cmd idle time 300

See also: [Idle Time]

Firmware revision R2.0.4-2571

igncond *n a*

Sets the condition(s) that would trigger an ignition report.
The state of the ignition is controlled by the "white" wire of the 3 wire power connection.

n = 1 to 8	ignition condition number
a = 0	trigger disabled (default)
a = 1	trigger on ignition going OFF
a = 2	trigger on ignition going ON
a = 3	trigger on transition (ON->OFF or OFF->ON)

Examples:

1. Set ignition condition 1 to trigger when ignition is going OFF :
   cmd igncond 1 1
1. Set ignition condition 2 to trigger when an ignition transition (ON to OFF or OFF to ON) is detected :
   cmd igncond 2 3

See Also: [Ignition Reports]

ignreport *[n] [r1] [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for ignition triggered reports.
Up to 8 ignition triggers can be configured, each supporting up to 8 reports.

n = 1 to 8	ignition trigger condition
r1 to r8 = 1 to 999	report number

Notes:

- When sending ignition reports remotely, ignition reports will be stored on the CTM-200 until a signal is obtained. For the stored reports to be sent, the following conditions must be met:
  - the CTM-200 must obtain a signal
  - **(Only applies to firmware below 3041)** The same report number(s)**(r1 to r8)** used in this command must be used in another command (ie. [obdreport], [vccreport])
  - **(Only applies to firmware below 3041)** The 'other' command (ie. [obdreport], [vccreport]) must be sending live data

---

Examples:

1. Set report #2 and #5 for ignition trigger condition #1 :
   cmd ignreport 1 2 5

See Also: [Ignition Reports]

input

Reads the value and state of all inputs. There are a total of six inputs on CTM200r1 and eight inputs on CTM200r2.
Both the analog voltage (range 0 to 10 Volts) and digital state (0 for off and 1 for on) are returned.

Notes:

- This is a read only command.

Examples:

1. Query the current status of input #1 through #6 :
   cmd input

See also: [General Purpose IO]

insetup *n d x.x p a*

Configures the six or eight inputs. Their use as a digital or analog input can be set along with their alarm states.

n = 1 to 6	input channel number (1 to 8 for CTM200r2)
d = A	set as analog input
d = D	set as digital input
x.x = 0 to 9.9	sets the voltage threshold for alarm reporting (valid if input set as analog only, use 0.0 for digital input)
p = P	sets input polarity to positive (this also determines the alarm level)
p = N	sets input polarity to negative (this also determines the alarm level)
a = 0	alarm off
a = 1	alarm on
a = 2	alarm on change state (valid for both digital and analog inputs - **CTM200 only**)

Notes:

- Voltage threshold values are accurate to one decimal place, (X.X), if additional decimal place values are entered, they will be rounded to the nearest decimal place.
- When configuring this command with a **digital** input, the voltage threshold parameter is ignored. The modem's I/O module has fixed digital input thresholds of 3 V and 2 V (1 V hysteresis).

Examples:

1. Set input #2 as *digital*, with *alarm* when *ON* :
   cmd insetup 2 D 0.0 P 1
1. Set input #4 as *analog*, with *alarm* when > *7.5V* :
   cmd insetup 4 A 7.5 P 1

See also: [General Purpose IO], [IO Reports]

Firmware revision 2.0.1.2221

ioaddmes *n x [x2][x3][x4]*

Adds a message to an IO report

n = 1 to 8	IO report number
x	message type to be added, valid message types must be used - see [message list]

Notes:

- Binary messages MUST be placed before ASCII messages. Ex. **cmd ioaddmes 1 85 114** = correct, **cmd ioaddmes 1 114 85** = incorrect.

Examples :

1. add message type #16 ? GPS NMEA GLL ? to IO report #4 :
   cmd ioaddmes 4 16

See also: [IO Reports]

iocond *n b t i1 i2 IP mt*

Sets the condition(s) that would trigger an IO report.

n = 1 to 8	IO report number
b = 0	conditional operator for the following parameters: Off (**Default**)
b = 1	conditional operator for the following parameters: AND
b = 2	conditional operator for the following parameters: OR
t = 0	timeout disabled
t = 1 to 65535	timeout in seconds
i1 = 0	alarm on input trigger: disabled
i1 = 1 to 6	alarm on input trigger: input number (1 to 8 for CTM200r2)
i2 = 0	alarm on input trigger: disabled
i2 = 1 to 6	alarm on input trigger: input number (1 to 8 for CTM200r2)
IP = 0	report if change in IP address: disabled
IP = 1	report if change in IP address: enabled
mt = 0 to 65535	maximum reporting rate in seconds (minimum time between reports)

Examples:

1. send report #1 every 60 seconds :
   cmd iocond 1 1 60
2. send report #2 every 60 seconds if input #1 is in alarm :
   cmd iocond 2 1 60 1
3. send report #3 every 60 seconds if inputs #1 and #2 are in alarm :
   cmd iocond 3 1 60 1 2
4. send report #4 whenever the IP address of the modem changes ? this indicates that it has made a new network connection :
   cmd iocond 4 2 0 0 0 1
5. send report #5 every 60 seconds or while input #3 is in alarm but with a maximum report rate of one every 10 seconds :
   cmd iocond 5 2 60 0 3 0 10
6. send report #6 only while input #6 is in alarm but with a maximum report rate of one every 10 seconds :
   cmd iocond 6 1 0 6 0 0 10

See also: [IO Reports]

iodelmes *n x*

Deletes a message (or all messages) from an IO report.

n = 1 to 8	IO report number
x	message type to be deleted or 0 to delete all messages

Examples:

1. deletes message type #16 from IO report #1 :
   cmd iodelmes 1 16
2. deletes all messages from IO report #4 :
   cmd iodelmes 4 0

See also: [IO Reports]

ioemail *n emailaddr*

Sets the email address that the IO report will be sent to (if configured for email using [iorep]).

n = 1 to 8	IO report number
emailaddr = name@domain	email address to which the report will be sent

Notes:

- An email server is required ? see [emailsrv]

Examples:

1. sets the send to email address for IO report #1 :
   cmd ioemail 1 me@?

See also: [IO Reports]

iolocip *n iii.iii.iii.iii*

Sets the IP address of the local server that the IO report will be sent to. Up to 8 IO reports can be configured.

n = 1 to 8	IO report number
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	local IP address in decimal (default: **192.168.1.20**)

Notes:

- **firmware 3396** and later can broadcast local UDP messages.

Examples:

1. Report #1 will be sent to local IP address 192.168.1.21 :
   cmd iolocip 1 192.168.1.21
2. Report #2 will be broadcasted on the local 192.168.1.0/24 subnet (**firmware 3396 and later**) :
   cmd iolocip 2 192.168.1.255

See also: [IO Reports]

Firmware revision R1.3.0.1967

iolocport *n xxxxx*

Sets the port number of the local server that the IO report will be sent to. Up to 8 IO reports may be configured.

n = 1 to 8	IO report number
xxxxx = 0 to 65535	local port number

Examples:

1. report #1 will be sent to local port 5005
   cmd iolocport 1 5005

See also: [IO Reports]

iomes

Displays all messages associated with each IO report.

Notes:

- This is a read only command.

Examples:

1. display all messages associated with each IO report :
   cmd iomes

See also: [IO Reports]

ioremip *n iii.iii.iii.iii*

Set the IP address of the remote server that the IO report will be sent to. Up to 8 IO reports may be configured.

n = 1 to 8	IO report number
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	remote IP address in decimal

---

Examples:

1. report #1 will be sent to remote IP address 123.10.1.101 :
   cmd ioremip 1 123.10.1.101

See also: [IO Reports]

ioremport *n xxxxx*

Sets the IP port number of the remote server that the IO report will be sent to. Up to 8 IO reports may be configured.

n = 1 to 8	IO report number
xxxxx = 0 to 65535	remote port number

Examples:

1. report #1 will be sent to port 5005 on remote IP address set by [ioremip] :
   cmd ioremport 1 5005

See also: [IO Reports]

iorep *n l r s*

Sets the reporting type for each IO report for the local and remote servers.

n = 1 to 8	IO report number
l = 0	disables the local report (default)
l = 1	asynchronous NMEA or ULCP messages over RS232
l = 2	asynchronous NMEA or ULCP messages with a ULCP header over RS232
l = 3	in-band NMEA or ULCP messages in a UDP Packet over Ethernet **Firmware 3211 and below**
l = 3	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets over Ethernet **Firmware 3232 and above**
l = 4	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets over Ethernet sent in binary format only
l = 5	in-band NMEA or ULCP messages in a TCP Packet over Ethernet **Firmware 3211 and below**
l = 5	in-band NMEA or ULCP messages with a ULCP header in individual TCP Packets over Ethernet **Firmware 3232 and above**
l = 6	file-based reports
r = 0	disables the remote report (default)
r = 3	in-band NMEA or ULCP messages in a UDP Packet **Firmware 3211 and below**
r = 3	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets **Firmware 3232 and above**
r = 4	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets in binary format only
r = 5	in-band NMEA or ULCP messages in a TCP Packet **Firmware 3211 and below**
r = 5	in-band NMEA or ULCP messages with a ULCP header in individual TCP Packets **Firmware 3232 and above**
r = 6	email reports
r = 7	SMS reports
s = 0	disables the store and forward of IO reports
s = 1	enables the store and forward of IO reports

Notes:

- For **r = 7** (SMS reports), the total length of the report must not exceed 166 characters including <CR> and <LF>
- A remote report cannot be configured when using **l = 6** (File-based reporting).

Examples:

1. send IO report #4 as a UDP packet over Ethernet and over the wireless link :
   cmd iorep 4 3 3
2. send IO report #2 as a UDP packet over Ethernet and as an SMS message to the SMS destination set using the [iosms] command, and enable the store and forward :
   cmd iorep 2 3 7 1
3. send IO report #5 as a TCP packet over the wireless link :
   cmd iorep 5 0 5

See also: [IO Reports]

iosms *n ppppppppppp|emailaddr*

Sets the destination of the IO report that is sent as an SMS message. Up to 8 IO reports may be configured. The default SMS destination is blank.

n = 1 to 8	IO report number
ppppppppppp	phone number which the SMS report will be sent to. For long distance numbers, a ?1? needs to be added In front of the phone number.
emailaddr	email address which the SMS report will be sent to.

Notes:

- SMS features are only available for specific manufacturer, RF modules, cards or devices. Please contact Cypress Solutions for a complete list of products that support SMS functionality.

Examples:

1. send IO report #1 as an SMS message to the specified phone number :
   cmd iosms 1 1234567890
2. sends IO report #2 as an SMS message to the specified email address :
   cmd iosms 2 me@?

See also: [IO Reports]

ipadr

Queries the IP address assigned to the modem by the wireless network.

Notes:

- This is a read only command.

Examples:

1. Query the current IP address of the modem :
   cmd ipadr

See also: [Diagnostics and Logging]

ipsec

Show all IPsec commands.

Notes:

- This is a read only command.

Examples:

1. show all IPsec commands :
   cmd ipsec

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec dpddelay *n*

This option activates the DPD (Dead Peer Detection) and sets the time (in seconds) allowed between 2 proof of liveliness requests.

n = 0	disables DPD monitoring, but still negotiates DPD support.(**Default**)
n = 1 to 3600	defines the DPD delay in seconds.

Examples:

1. Set DPD delay time to 300 seconds :
   cmd ipsec dpddelay 300

See also: [IPsec]

ipsec dpdmaxfail *n*

If cmd ipsec dpddelay is set > 0, this sets the maximum number of liveliness proofs to request (without reply) before considering the peer is dead.

n = 0 to 100	defines the DPD maxfail count, **default value is 5**.

Examples:

1. Set DPD maximum number of proof requests to 10 :
   cmd ipsec dpdmaxfail 10

See also: [IPsec]

ipsec dpdretry *n*

If this command is set, this sets the delay to wait for a proof of liveliness before considering it as failed and send another request.

n = 0 to 3600	defines the DPD retry in seconds. (**Default 5**)

Examples:

1. Set DPD retry to 10 seconds :
   cmd ipsec dpdretry 10

See also: [IPsec]

ipsec enable *n*

Enable/disable IPsec on the CTM-200.

n = 1	enable IPsec
n = 0	disable IPsec

Examples:

1. Enable IPsec on the CTM-200 :
   cmd ipsec enable 1

See also: [IPsec]

ipsec ikeauth psk

Defines the authentication method used for the phase 1 negotiation.
Currently pre-shared key is the only supported authentication method.

See also: [IPsec]

ipsec ikedhgroup *n*

Define the IPsec IKE phase I Diffie-Hellman group.

n = 1	modp768
n = 2	modp1024 (**default**)
n = 5	modp1536
n = 14	modp2048
n = 15	modp3072
n = 16	modp4096
n = 17	modp6144
n = 18	modp8192

Examples:

1. Set the IPsec IKE phase I Diffie-Hellman group to modp2048 :
   cmd ipsec ikedhgroup 14

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec ikeenc *alg*

Define the IPsec IKE phase I encryption algorithm.

alg = des	Data Encryption Standard algorithm
alg = 3des	Triple DES algorithm (default)
alg = aes	Advanced Encryption Standard algorithm
alg = aes256	Advanced Encryption Standard (256-bit key) algorithm

---

Examples:

1. Set the IPsec IKE phase I encryption algorithm to DES :
   cmd ipsec ikeenc des

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec ikeexchange *mode*

Define the IPsec IKE phase I exchange mode when the peer is configured as an initiator (client).

mode = main	Main mode (**default**)
mode = aggressive	Agressive mode

Examples:

1. Set the IPsec IKE phase I exchange mode to aggressive mode :
   cmd ipsec ikeexchange aggressive

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec ikehash *alg*

Define the IPsec IKE phase I hash algorithm.

alg = md5	Message-Digest algorithm 5 (MD5) hash algorithm
alg = sha1	Secure Hash Algorithm-1 (SHA-1) hash algorithm (default)

The current setting can be queried by entering the **ipsec ikehash** command without parameters.

Examples:

1. Set the IPsec IKE phase I hash algorithm to MD5 :
   cmd ipsec ikehash md5

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec ikeinitial *n*

Define the IPsec IKE phase I initial contact setting. Enable this to set the IPsec daemon to send an INITIAL-CONTACT message.

n = 0	set initial contact on (**default**)
n = 1	set initial contact off

Examples:

1. Set the IPsec IKE phase I initial contact setting off :
   cmd ipsec ikeinitial 0

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec ikelifetime *n*

Define the IPsec IKE phase I lifetime in seconds.

n = 0 to 268435455	IKE phase 1 lifetime in seconds (default: 3600 s)

Examples:

1. Set the IPsec IKE phase I lifetime to 2 h (7200 s) :
   cmd ipsec ikelifetime 7200

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec ikemodecfg *n*

Gather network information through ISAKMP mode configuration. Default is off

n = 0	**off** (Default)
n = 1	**on**

See also: [IPsec]

ipsec ikemyid type value

Specifies the identifier sent to the remote host and the type to use in the phase 1 negotiation: address, fqdn, user_fqdn

type	
address	where value is the IP address. (Default)
user_fqdn value	where value is a USER_FQDN (user fully-qualified domain name)
fqdn value	where value is a FQDN (fully-qualified domain name)

Examples:

1. Set the IPsec local identifier to an IP address :
   cmd ipsec ikemyid address 99.88.77.66

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec ikepassive *n*

Define the IPsec IKE phase I peer role of the modem as either initiator or responder.

n = 0	set passive off, setting modem as IPsec initiator (client) (default)
n = 1	set passive on, setting modem as IPsec responder (server)

Examples:

1. Set the IPsec passive setting on :
   cmd ipsec ikepassive 1

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec ikepeerid type value

Specifies the identifier to be received from the remote host in the phase 1 negotiation: address, fqdn, user_fqdn

type	
address	where value is the IP address. (Default)
user_fqdn value	where value is a USER_FQDN (user fully-qualified domain name)
fqdn value	where value is a FQDN (fully-qualified domain name)

Examples:

1. Set the IPsec local identifier to an IP address :
   cmd ipsec ikepeerid address 88.88.88.88

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec ikeproposal obey|strict|claim|exact

Specifies the action of lifetime length, key length, and PFS of the phase 2 selection on the responder side, and the action of lifetime check in phase 1.

obey	The responder will obey the initiator anytime(**default**).
strict	If the responder's lifetime length is not equal to the initiator's, the responder will use the initiator's value. Otherwise, the proposal will be rejected. If PFS is not required by the responder, the responder will obey the proposal. If PFS is required by both sides and the responder's group is not equal to the initiator's, then the responder will reject the proposal.
claim	If the responder's lifetime length is not equal to the intiator's, the responder will use the initiator's value. If the responder's lifetime length is shorter than the initiator's, the responder uses its own length AND sends a RESPONDER-LIFETIME notify message to an initiator in the case of lifetime (phase 2 only). For PFS, this directive behaves the same as strict.
exact	If the initiator's lifetime or key length is not equal to the responder's, the responder will reject the proposal. If PFS is required by both sides and the responder's group is not equal to the initiator's, then the responder will reject the proposal.

Examples:

1. Set IKE proposal check level to strict :
   cmd ipsec ikeproposal strict

See also: [IPsec]

ipsec ikerekey on|off|force

Enable automatic renegotiation of expired phase1 when there are non-dying phase2 SAs. Possible values are:

force	Rekeying is done unconditionally.
on	Rekeying is done only if DPD monitoring is active. (Default)
off	No automatic rekeying. Note that turning off automatic rekeying will result in inaccurate DPD monitoring.

Examples:

1. Force IPsec DPD rekeying :
   cmd ipsec ikerekey force

See also: [IPsec]

ipsec ikeverifyid n

If you want to verify the peer's identifier, set this to on. In this case, if the value defined by ikepeerid is not the same as the peer's identifier in the ID payload, the negotiation will fail.

n = 0	**off** : No peer ID verification (Default)
n = 1	**on** : Peer ID verification on

Examples:

1. Enable peer_identifier verification :
   cmd ipsec ikeverifyid 1

See also: [IPsec]

ipsec localnet *n*

Defines whether to use the CTM-200 eth0 or eth1 LAN ports for the local IPsec tunnel.

n=0	use LAN0 (eth0) for local IPsec tunnel (**default**)
n=1	use LAN1 (eth1) for local IPsec tunnel

Examples:

1. Set IPsec to use LAN1 :
   cmd ipsec localnet 1

See also: [IPsec]

ipsec loglevel info|notify|debug|debug2

Defines the IPsec logging level.

info	lowest log level (**default**)
debug2	highest log level

If you set the logging level too high, IKE negotiation can fail due to timing constraint changes.

Examples:

1. Set log level to notify :
   cmd ipsec loglevel notify

See also: [IPsec]

ipsec natt *n*

Enable IPsec NAT traversal (NAT-T) setting. NAT-T allows one or both peers to reside behind a NAT gateway (i.e. doing address- or port-translation).

n = 0	Disable IPsec NAT-T setting (**default**)
n = 1	Enable IPsec NAT-T setting

Examples:

1. Set the IPsec NAT-T setting as enabled :
   cmd ipsec natt 1

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec nattkeepalive *n*

Set the IPsec NAT traversal (NAT-T) keepalive interval. This is the interval between sending NAT-T keepalive packets.

n = 0	Disable sending of NAT-T keepalive packets
n = 1 to 3600	NAT-T keepalive interval in seconds (Default: 20 seconds)

Examples:

1. Set the IPsec NAT-T keepalive interval to 5 minutes (300 seconds) :
   cmd ipsec nattkeepalive 300

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec psk *iii.iii.iii.iii key*

Set IPsec pre-shared key used for IKE phase I.

iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	IP address of remote peer in decimal
key	Alpha-numeric pre-shared key

Notes:

- You should only use this command from a LAN connection
- To set a pre-shared key securely from a remote location, this command should only be used from within a SSH connection.

Examples:

1. Set the IPsec pre-shared key for remote IPsec peer with IP address of 1.2.3.4 to testPSK1234 :
   cmd ipsec psk 1.2.3.4 testPSK1234

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec rekey on|off|force

Enable automatic renegotiation of expired phase1 when there are non-dying phase2 SAs. Possible values are:

force Rekeying is done unconditionally.

on Rekeying is done only if DPD monitoring is active. This is the default.

off No automatic rekeying. Note that turning off automatic rekeying will result in inaccurate DPD monitoring.

The current setting can be queried by entering the **ipsec rekey** command without parameters.

Examples:

1. Force IPsec DPD rekeying

```
/ # cmd ipsec rekey force
OK
```

1. Query the current setting:

```
/ # cmd ipsec rekey
cmd ipsec rekey on
OK
```

ipsec remgw *iii.iii.iii.iii*

Define IPsec remote gateway IP address.

iii.iii.iii.iii = anonymous	When configured as IPsec responder (server), use this to accept IPsec connection proposals from all IP addresses
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	IP address of IPsec remote gateway in decimal

Examples:

1. Set the IPsec remote gateway IP address to 1.2.3.4 :
   cmd ipsec remgw 1.2.3.4

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec remnet *n iii.iii.iii.iii m*

Define IPsec remote subnet(s) using Classless Inter-Domain Routing (CIDR) notation.

n = 1 to 50	Subnet number
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	IP address of remote subnet in decimal
m = 1 to 32	Subnet mask represented in CIDR notation

Examples:

1. Set IPsec remote subnet 1 to 192.168.2.0/24 :
   cmd ipsec remnet 1 192.168.2.0 24

See also: [IPsec]

The operation of this command has been verified in 1.3.0.1994

ipsec remping *n*

Set interval to ping a remote target specified using the [ipsec remtarget] command.

n	ping time interval (seconds)

Examples:

1. ping the remote target every 30 seconds :
   cmd ipsec remping 30

See also: [IPsec]

ipsec remtarget *iii.iii.iii.iii*

Specify remote IP address to periodically ping. Ping interval is specified using [remping] command

iii.iii.iii.iii = 0.0.0.0 - 255.255.255.255	remote target IP address

---

Examples:

1. Specify remote target address of 75.182.111.70 :
   cmd ipsec remtarget 75.182.111.70"

See also: [IPsec]

ipsec restrict *n*

Set restrictive access policy for IPsec applications. Enabling the restrictive access policy limits all traffic from the modem to the IPsec subnet(s) and the remote IPsec peer.

n = 0	Disable restrictive access policy for IPsec applications (**default**)
n = 1	Enable restrictive access policy for IPsec applications

Notes:

- At least one IPsec remote subnet must be configured using [ipsec remnet] for this setting to take effect.
- Remote access via Telnet, SSH, or embedded Web interface is not possible when **cmd ipsec restrict 1** is configured.

Examples:

1. Enable the restrictive IPsec access policy :
   cmd ipsec restrict 1

See also: [IPsec]

The operation of this command has been verified in 1.3.0.1994

ipsec saauth *alg*

Define the IPsec ISAKMP phase II authentication algorithm.

alg = hmac_md5	Message-Digest algorithm 5 (MD5) authentication algorithm
alg = hmac_sha1	Secure Hash Algorithm-1 (SHA-1) authentication algorithm (default)

Examples:

1. Set the IPsec ISAKMP phase II authentication algorithm to MD5 :
   cmd ipsec saauth md5

See also: [IPsec]

Firmware revision 1.3.0.1994

ipsec saenc *alg*

Define the IPsec ISAKMP phase II encryption algorithm.

alg = des	Data Encryption Standard algorithm
alg = 3des	Triple DES algorithm (default)
alg = aes	Advanced Encryption Standard algorithm
alg = aes256	Advanced Encryption Standard (256-bit key) algorithm

---

Examples:

1. Set the IPsec ISAKMP phase II encryption algorithm to DES :
   cmd ipsec saenc des

See also: [IPsec]

The operation of this command has been verified in 1.3.0.1994

ipsec salifetime *n*

Define the IPsec ISAKMP phase II lifetime in seconds.

n = 0 to 268435455	ISAKMP phase II lifetime in seconds (default: 3600 s)

Examples:

1. Set the IPsec ISAKMP phase II lifetime to 2 h (7200 s) :
   cmd ipsec salifetime 7200

See also: [IPsec]

The operation of this command has been verified in 1.3.0.1994

ipsec sapfsgroup *n*

Define the IPsec ISAKMP perfect forward secrecy group.

n = 0	none
n = 1	modp768
n = 2	modp1024 (default)
n = 5	modp1536
n = 14	modp2048
n = 15	modp3072
n = 16	modp4096
n = 17	modp6144
n = 18	modp8192

Examples:

1. Set the IPsec ISAKMP perfect forward secrecy group to modp2048 :
   cmd ipsec sapfsgroup 14

See also: [IPsec]

The operation of this command has been verified in 1.3.0.1994

ipsec show

Show IPsec configuration.

Notes:

- This is a read only command.

Examples:

1. show IPsec commands :
   cmd ipsec show

See also: [IPsec]

The operation of this command has been verified in 1.3.0.1994

ipsec split *n*

Enable/disable IPsec split-tunneling on the CTM-200.

n = 0	disable split-tunnel
n = 1	enable split-tunnel (**default**)

Notes:

- when split-tunnel is disabled, ALL outgoing traffic from the CTM-200 will be routed through the IPsec tunnel.
- when split-tunnel is disabled, **ONLY ONE** remote subnet should be defined. ie. cmd ipsec remnet 2..10 should all be **0.0.0.0 0**.
- when split-tunnel is disabled A PC on the remote side of the tunnel will not be able to access PC/devices on the LAN side of the CTM-200.
- when split-tunnel is disabled, the CTM-200 cannot access PC/devices on the LAN side of the CTM-200.

Examples:

1. Disable split-tunneling on the CTM-200 IPsec:
   cmd ipsec split 0

See also: [IPsec]

Firmware revision 2.0.5.3034

lanbridge *n*

Enable bridging of LAN ports on CTM-200. When bridging is enabled, both LAN ports will be bridged to a common IP address, this allows PC devices connected to LAN0 and LAN1 to see each other on the same LAN subnet.

n = 0	disabled **(default)**
n = 1	enabled

Notes:

- A static IP address must be defined for LAN0.

Example:

1. enable lanbridge :
   cmd lanbridge 1

See also: [LAN]

Firmware revision 2.0.5.2968

landhcp *p ddd n*

Configures the LAN dynamic host configuration protocol (DHCP) server settings on the CTM-200 gateway, specifically the starting IP address to assign to DHCP users and the maximum number of DHCP users on the LAN.

p = 0 or 1	ethernet port
ddd = 0 to 255	Starting DHCP IP address to be leased. **ddd** is referring to the last ipv4 octet (ie. aaa.bbb.ccc.**ddd**). Use **0** to disable. (**default 20**).
n = 1 to 254	Maximum number of DHCP clients. Use **0** to disable. (**default 10**)

Examples:

1. Assign DHCP address range from 192.168.1.**20** to 192.168.1.**35** to LAN0 DHCP clients
   cmd lanip 0 192.168.1.1
   cmd landhcp 0 20 15
1. Assign DHCP address range from 192.168.10.**15** to 192.168.10.**25** to LAN1 DHCP clients
   cmd lanip 1 192.168.10.1
   cmd landhcp 1 15 10
1. Disable DHCP on LAN0
   cmd landhcp 0 0 0

See also: [DHCP]

landns *p iii.iii.iii.iii [jjj.jjj.jjj.jjj]*

Set DNS nameserver IP address(es) for the CTM-200 LAN client interfaces.

p = 0 or 1	ethernet port
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	Primary DNS IP address in decimal (default for **eth0** is **192.168.1.1**. Default for **eth1** is **192.168.2.1**)
jjj.jjj.jjj.jjj = 0.0.0.0 to 255.255.255.255	Secondary DNS IP address in decimal (optional) (default for **eth0** is **192.168.1.1**. Default for **eth1** is **192.168.2.1**)

Note:

- **cmd landns** should only be set if using **cmd lanproto static**.

Examples:

1. Set the eth0 DNS nameserver IP address to **192.168.10.254**:
   cmd landns 0 192.168.10.254
1. Set the eth1 DNS nameserver IP addresses to **192.168.10.253** and **192.168.10.254**:
   cmd landns 1 192.168.10.253 192.168.10.254

See also: [LAN]

lanfriends *n xx:xx:xx:xx:xx:xx*

This command is used to control access to PC devices connected through the CTM-200 ethernet ports.
Define up to 8 MAC addresses that are allowed ethernet access, all other devices will be denied packet forwarding/routing

n = 1 to 8	lanfriends list number
xx:xx:xx:xx:xx:xx	MAC address of PC to allow access. Use 0 to reset/disable

---

Examples:

1. ethernet access granted to PC with ethernet MAC address 00:A0:D2:69:B2:C8 :
   cmd lanfriends 1 00:A0:D2:69:B2:C8

See also: [Friends List]

Firmware revision 2.0.5.2968

langw *p iii.iii.iii.iii*

Set default gateway IP address for the CTM-200 LAN client interfaces.

p = 0 or 1	ethernet port
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	gateway IP address in decimal (default: **eth0: 192.168.1.1** and **eth1: 192.168.2.1**)

Notes:

- **cmd langw** should only be set if using **cmd lanproto static**.

Examples:

1. Set the eth0 default gateway IP address to 192.168.10.254 :
   cmd langw 0 192.168.10.254

See also: [LAN]

lanip *p iii.iii.iii.iii [mmm.mmm.mmm.mmm]*

Sets the IP address of the CTM-200 gateway's ethernet ports.

p = 0 or 1	ethernet port to configure (eth0/lan0 or eth1/lan1)
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	LAN IP address of the ethernet port in decimal (default: **eth0: 192.168.1.1** and **eth1: 192.168.2.1**)
mmm.mmm.mmm.mmm = 0.0.0.0 to 255.255.255.255	LAN netmask of the ethernet port in decimal (default: **255.255.255.0**)

Note:

- Special care must be taken when configuring this command, if an improperly configured lanip IP address is entered the ethernet port can be rendered unusable. Before configuring this command it is advisable to make sure that a command console is available via the serial port, or the IP address is known and remote ssh/telnet is enabled to allow the gateway to be accessed wirelessly.

Examples:

1. Set the LAN IP address of the eth1 port to 192.168.10.1 :
   cmd lanip 1 192.168.10.1
2. Set the LAN IP address of the eth1 port to 192.168.2.1 and netmask to 255.255.0.0 :
   cmd lanip 1 192.168.2.1 255.255.0.0

See also: [LAN]

lannat *p n*

Enables NAT (Network Address Translation) on the CTM-200 ethernet port(s). This configuration would be used for the case where an ethernet port is connected to the Internet.

p = 0 or 1	ethernet port to configure (eth0/lan0 or eth1/lan1)
n = 0	NAT disabled
n = 1	NAT enabled

Examples:

1. Enable NAT on ethernet port 0 :
   cmd lannat 0 1

See also: [LAN]

lannetmask *p iii.iii.iii.iii*

Sets the netmask of the CTM-200 gateway's ethernet port on the LAN.

p = 0 or 1	ethernet port to configure (eth0/lan0 or eth1/lan1)
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	LAN netmask of the gateway in decimal (default: **255.255.255.0**)

Notes:

- Special care must be taken when configuring this command, if an improperly configured lannetmask IP address is entered the ethernet port can be rendered unusable. Before configuring this command it is advisable to make sure that a command console is available via the serial port, or the IP address is known and remote ssh/telnet is enabled to allow the gateway to be accessed wirelessly.

Examples:

1. Set the LAN netmask of the CTM-200 gateway's eth1 port to 255.255.0.0 :
   cmd lannetmask 1 255.255.0.0

See also: [LAN]

lanproto *p type*

Configure LAN interface protocol on LAN0 or LAN1 to use DHCP or a Static IP address.

p = 0 or 1	Lan port LAN0 = 0, LAN1 = 1
type = static	IP address of CTM-200 LAN port will be statically configured - see [lanip]
type = dhcp	IP address of CTM-200 LAN port will be assigned by a DHCP server

---

Examples:

1. Set eth0 for static IP address :
   cmd lan 0 proto static
1. eth1 will receive IP address from a DHCP server :
   cmd lan 1 proto dhcp

See also: [LAN]

lanrepip *iii.iii.iii.iii*

Sets the IP address of the local server connected to the modem?s LAN that will receive local reports.

iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	LAN IP address to receive local reports in decimal (default: **192.168.1.20**)

Examples:

1. Set the local reporting LAN IP address to 192.168.1.21 :
   cmd lanrepip 192.168.1.21

See also: [LAN]

Firmware revision 1.2.0_RC8

lanwd*n*

Enable / disable the LAN watchdog. The LAN watchdog is used to monitor for potential ethernet / ARP issues.

n = 0	disabled
n = 1	enabled **(default)**

Notes:

Example:

1. Disable LAN watchdog :
   cmd lanwd 0

See also: [LAN]

Firmware revision 2.0.5.3201

mbusm add *n ip|serial*

This is command is used when the CTM200 is being used as a MODBUS Master

Command is used when CTM-200 is being used as a MODBUS Master device and polling MODBUS Slave device through TCP or Serial port. This command will add a MODBUS Slave to MODBUS Master polling list. It will display all MODBUS slaves to be polled when it is used without arguments.

n = 1 to 4	MODBUS Slave device ID
ip = 1.0.0.0 to 255.255.255.255	Add MODBUS TCP slave type. MODBUS Slave Device IP address
serial = Serial A or **Serial a**	Add MODBUS Serial slave type. MODBUS Slave using ASCII protocol
serial = Serial R or **Serial r**	Add MODBUS Serial slave type. MODBUS Slave using RTU protocol

---

Examples:

1. Query the current list :
   cmd mbusm add
1. Add a MODBUS serial slave device that uses ASCII protocol :
   cmd mbusm add 1 Serial A
1. Add MODBUS TCP slave devices that has an IP of 192.168.100.100 and .101 :
   cmd mbusm add 2 192.168.100.100
   cmd mbusm add 3 192.168.100.101

See also: [MODBUS]

Firmware revision 2.0.4.2702

mbusm cond *n b t [sid1, r1, dt1, md1, Md1] [sid2, r2, dt2, md2, Md2] [mt]*

This is command is used when CTM200 is being used as a MODBUS Master

Set the condition that will trigger a MODBUS Master report. The conditional operator is used to indicate how all of the following parameters will be used to determine if a report is triggered.

n = 1 to 8	MODBUS Master trigger condition number
b = 0	Conditional operator for all parameters: Off (**default**)
b = 1	Conditional operator for all parameters: AND
b = 2	Conditional operator for all parameters: OR
t = 0	Timeout disabled (**default**)
t = 1 to 65535	Timeout in seconds
sid1 = 0	Disable comparing register r1 of sid1 (**default**)
sid1 = 1 to 4	MODBUS Slave device ID
r1 = 0	Disable comparing register r1 of sid1 (**default**)
r1 = 1 to 65536	Register address in sid1
dt1 = 0	Data type: Single bit, discrete output (**default**)
dt1 = 1	Data type: Single bit, discrete input
dt1 = 2	Data type: 2 bytes, 16-bit register input
dt1 = 3	Data type: 4 bytes, 32-bit integer input
dt1 = 4	Data type: 4 bytes, 32-bit float input
dt1 = 5	Data type: 2 bytes, 16-bit register output
dt1 = 6	Data type: 4 bytes, 32-bit integer output
dt1 = 7	Data type: 4 bytes, 32-bit float output
md1	Low data value of r1. Data type is defined by dt1 (**0 is default**)
Md1	High data value of r1. Data type is defined by dt1 (**0 is default**)
sid2 = 0	Disable comparing register r2 of sid2 (**default**)
sid2 = 1 to 4	MODBUS Slave device ID
r2 = 0	Disable comparing register r2 of sid2 (**default**)
r2 = 1 to 65536	Register address in sid2
dt2	The same as **dt1**
md2	Low data value of r2. Data type is defined by dt2 (**0 is default**)
Md2	High data value of r2. Data type is defined by dt2 (**0 is default**)
mt = 0 to 65535	Maximum reporting rate in seconds (minimum time between reports) (**0 is default**)

Notes:

- The **mt** parameter must be used at the end if all other optional parameters are entered.

Examples:

1. Send MODBUS Master report 1 every 60 seconds :
   cmd mbusm cond 1 1 60

1. Send MODBUS Master report 2 every 60 seconds AND if register 2 of MODBUS Slave 1 is between 10 and 20 :
   cmd mbusm cond 2 1 60 1 2 5 10 20
1. Send MODBUS Master report 3 every 60 seconds OR if register 2 of MODBUS Slave 1 is between 10 and 20, OR if register 3 of MODBUS Slave 4 is between 100 and 200, with a maximum report rate of one report every 10 seconds :
   cmd mbusm cond 3 2 60 1 2 5 10 20 4 3 5 100 200 10
1. Query the conditions used to trigger all MODBUS Master reports :
   cmd mbusm cond
1. Query the conditions used to trigger MODBUS Master report 2 :
   cmd mbusm cond 2

See also: [MODBUS]

Firmware revision 2.0.4.2702

mbusm data *n*

This is command is used when CTM200 is being used as a MODBUS Master

Show the current register values from a MODBUS slave to debug the device status.

n = 1 to 4	MODBUS Slave device ID

Examples:

1. Show current register values from MODBUS slave ID #2 :
   cmd mbusm data 2

See also: [MODBUS]

Firmware revision 2.0.4.2702

mbusm del *n*

This is command is used when CTM200 is being used as a MODBUS Master

This command deletes one or all MODBUS slaves from MODBUS Master polling list.

n = 0	Delete all MODBUS slaves
n = 1 to 4	Delete specific MODBUS Slave device

Examples:

1. Delete MODBUS slave ID #3 from MODBUS Master polling list :
   cmd mbusm del 3

See also: [MODBUS]

Firmware revision 2.0.4.2702

mbusm exccond *e*

This is command is used when CTM200 is being used as a MODBUS Master

Set the condition that will trigger MODBUS exception reports.

e = 0	Disable the MODBUS exception reports (**default**)
e = 1 to 7FFF in hex	MODBUS events and exceptions to be used

MODBUS Event and Exception Bitmap:

bit0	**Illegal Function Exception, Code 1** A master sends a Modbus function, which is not supported by the slave device.
bit1	**Illegal Address Exception, Code 2** A master queries an invalid or non-existing data address.
bit2	**Illegal Value Exception, Code 3** A master sends a data value, which is not an allowable value for the slave device.
bit3	**Slave Failure Exception, Code 4** An unrecoverable error occurs in the slave device. The length might exceed the allowable data size.
bit4	**Acknowledge Exception, Code 5** A long duration of time will be required to process the request. This is to prevent a timeout error.
bit5	**Slave Device Busy Exception, Code 6** A long?duration program command is running. The command should be retransmitted later.
bit6	**NAK Exception, Code 7** The slave cannot perform the program function received in the query.
bit7	**Memory Parity Error Exception, Code 8** A master attempted to read record file, but detected a parity error in the memory.
bit8	**Gateway Path Unavailable Exception, Code 10/0x0A** The gateway is unable to establish a connection with the target device.
bit9	**Gateway Target Fail Exception, Code 11/0x0B** The gateway is unable to receive a response from the target device. Usually means that the device is not present on the network.
bit10	**Reply Timeout Event, Code 12/0x0C** The slave device does not reply in time or does not reply at all. The device ID might be wrong.
bit11	**Send Timeout Event, Code 13/0x0D** The handshake lines are not properly set.
bit12	**Device Open Error Event, Code 14/0x0E** The Modbus Master couldn't open a serial or TCP slave device. The network is down, or the serial port is already opened. The function code in $PMEX will be 0 for this event.
bit13	**TCPIP Connection Closed Event, Code 15/0x0F** TCP/IP connection was closed by the remote slave device.
bit14	**Unknown Poll Error Event, Code 16/0x10** This event is for all other errors when polling slave devices.

At least one event or exception defined by **e** should be detected to trigger reports. The exception code **12 ~ 16** are defined by Cypress Solutions.

See also: [MODBUS]

Firmware revision 2.0.4.2702

mbusm excreport *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This is command is used when CTM200 is being used as a MODBUS Master

Set the reports to be used for MODBUS exception triggered reports. The message $PMEX will be appended after each generic report

r1...r8 = 0	Disables the report (**default**)
r1...r8 = 1 to 999	Report number

See also: [MODBUS], [General Reports]

Firmware revision 2.0.4.2702

mbusm poll *n r c [dt] [f] [o] [e]*

This is command is used when CTM200 is being used as a MODBUS Master

Configure polling MODBUS slaves.

n = 1 to 4	MODBUS Slave device ID
r = 0	Reset the configuration and disable polling (**default**)
r = 1 to 65536	Start register address
c = 1 to 50	Number of registers to be read (**1 is default**)
dt = 0	Data type: Single bit, discrete output
dt = 1	Data type: Single bit, discrete input
dt = 2	Data type: 2 bytes, 16-bit register input
dt = 3	Data type: 4 bytes, 32-bit integer input
dt = 4	Data type: 4 bytes, 32-bit float input
dt = 5	Data type: 2 bytes, 16-bit register output (**default**)
dt = 6	Data type: 4 bytes, 32-bit integer output
dt = 7	Data type: 4 bytes, 32-bit float output
f = 1 to 10000	Poll rate in ms (**1000 is default**)
o = 1 to 10000	Slave timeout in ms (**1000 is default**)
e = 0	Little-endian (**default**)
e = 1	Big-endian

Examples:

1. Poll MODBUS slave device 2 every 1 second, starting from register 4 to register 13 (10 registers). Data type is 2 bytes, 16-bit output :
   cmd mbusm poll 2 4 10 5 1000 1000 0

See also: [MODBUS]

Firmware revision 2.0.4.2702

mbusm report *n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This is command is used when CTM200 is being used as a MODBUS Master

Set the reports to be used for MODBUS Master triggered reports.

n = 1 to 8	MODBUS Master trigger condition
r1...r8 = 0	Disables the report (**default**)
r1...r8 = 1 to 999	Report number

See also: [MODBUS], [General Reports]

Firmware revision 2.0.4.2702

mip *n*

Sets the Mobile IP operation of the modem. This command is only applicable to CDMA/EV-DO devices.

n = 0	simple IP only (mobile IP disable)
n = 1	mobile IP preferred (default)
n = 2	mobile IP only

Examples:

1. sets the MIP option to be MIP preferred :
   cmd mip 1

See also: [Cellular]

modbusadd ***id [ip|serial]***

This is command is used when CTM200 is being used as a MODBUS Slave Gateway

id = 1 to 247	MODBUS ID. If **ip** and **serial** are blank, then this adds CTM itself as a slave (only one is permitted)
ip = 1.0.0.0 to 255.255.255.255	Adds a MODBUS TCP Slave (IP address of MODBUS devices connected to the modem's ethernet port)
serial = Serial A or **Serial a**	Adds a MODBUS Serial Slave using ASCII transmission mode
serial = Serial R or **Serial r**	Adds a MODBUS Serial Slave using RTU transmission mode

---

Examples:

1. Add TCP slave with ID 1 and IP 192.168.100.122 :
   cmd modbusadd 1 192.168.100.122
1. Add itself as a MODBUS slave with ID = 3 :
   cmd modbusadd 3

See also: [MODBUS]

Firmware revision 2.0.4.2702

modbusctm130 *n*

This is command is used when CTM200 is being used as a MODBUS Gateway

Enables MODBUS backward compatibility with the CTM-13X by using MODBUS RTU encapsulated in UDP packets for messages transmitted/received over-the-air.
The CTM-13X modems only use MODBUS RTU over UDP as the over-the-air protocol for communicating between other modems configured as MODBUS master and slave gateways.

n = 0	Use MODBUS TCP for over-the-air communications (**default**)
n = 1	Use MODBUS RTU over UDP for over-the-air communications

---

Examples:

1. Set MODBUS gateway to send/receive MODBUS RTU over UDP messages :
   cmd modbusctm130 1

See also: [MODBUS]

Firmware revision 2.0.1.2138

modbusdel *n*

This is command is used when CTM200 is being used as a MODBUS Gateway

Deletes an entry or all entries from the MODBUS list.

n = 0	Deletes all MODBUS entries
n = 1 to 247	MODBUS ID entry

Examples:

1. Delete the entry with MODBUS ID 1 :
   cmd modbusdel 1
1. Delete all entries inthe MODBUS list :
   cmd modbusdel 0

See also: [MODBUS]

Firmware revision 2.0.4.2702

modbusgw

This is command is used when CTM200 is being used as a MODBUS Gateway

Use this to initiate the MODBUS gateway manually from the serial port console.

Notes:

- FW rev R1.3.0 and above - [freeconsole] must be run first before using this command.

Examples:

1. Initiate the MODBUS gateway manually :
   cmd freeconsole
   cmd modbusgw

See also: [MODBUS], [cmd_freeconsole]

Firmware revision 1.3.0 (rev. 1640)

modbusidmap *n ip p*

This is command is used when CTM200 is being used as a MODBUS Master Gateway
This command sets up the MODBUS ID to modem IP for each remote MODBUS slave device (i.e. another CTM200/CTM15x modem configured as a MODBUS slave gateway).

n = 1 to 247	MODBUS ID, in decimal
ip = 0.0.0.0 to 255.255.255.255	MODBUS slave modem IP address in decimal (wireless modem IP address) (**0.0.0.0 is default**)
p = 0 to 65535	Port that the slave modem will be listening on, in decimal

---

Notes:

- This command returns ERROR if the modem is configured as a SLAVE GATEWAY (**cmd modbusmode 0**).

Examples:

1. Set the MODBUS master gateway to forward messages designated for the slave device with ID 1 to the modem at 123.1.2.3, port 502 :
   cmd modbusidmap 1 123.1.2.3 502

See also: [MODBUS]

Firmware revision 2.0.4.2702

modbusmode *n*

Configures the CTM to act as a MODBUS Master or MODBUS gateway. If configuring for MODBUS master gateway, can specify the transmission mode between the modem configured as the serial master gateway and the MODBUS serial device connected to the modem.

n = 0	MODBUS Gateway: Slave gateway (**default**)
n = 1	MODBUS Gateway: RTU master gateway
n = 2	MODBUS Gateway: ASCII master gateway
n = 3	MODBUS Master

Examples:

1. Set CTM to be a MODBUS serial RTU master gateway :
   cmd modbusmode 1
1. Set CTM to be a MODBUS master which will poll connected MODBUS slaves :
   cmd modbusmode 3

See also: [MODBUS]

Firmware revision 2.0.4.2702

modbusport *xxxxx*

This is command is used when CTM200 is being used as a MODBUS Gateway

Sets the listening port number for the MODBUS server and the listening port number for MODBUS TCP slaves.

xxxxx = 1 to 65535	MODBUS server port number (**default 502**)

Examples:

1. Set the MODBUS port to 12345 :
   cmd modbusport 12345

See also: [MODBUS]

Firmware revision 2.0.4.2702

modbussecure *n*

Secure access to the modem's MODBUS server from the Internet.
If enabled, it will not be possible to remotely access the MODBUS server via the port specified in [modbusport] and using the current IP address allocated to the CTM-200 by the network.
This is to support applications where the servers may be accessed through SSH tunneling.

n = 0	Allow direct access to MODBUS server from Internet (**default**)
n = 1	Secure - do not allow direct access to MODBUS server from Internet

---

Examples:

1. Set the CTM-200 to secure access to MODBUS server from Internet :
   cmd modbussecure 1

See also: [MODBUS]

Firmware revision 1.3.0.2090

mode *a b c*

Sets the required functionality of the serial ports.

a	The function of ttyAM0 (Primary DB9) (port 1)
b	The function of ttyAM1 (Secondary DB9) (port 2)
c	The function of ttyAM3 (RS485) (port 3)

Mode	Serial Port Function
1	None
2	Console
3	PPP
4	PAD host interface
6	MODBUS host interface
9	Magnetic Card Reader interface
10	WPAN Gateway
12	Chlorobyte Spreader Controller interface
13	external GPS receiver
15	Epomaster Spreader Controller interface
17	Garmin mode - client/server
18	Garmin mode - client only
19	Garmin mode - server only
20	WPAN PAD client loopback
21	Diagnostic passthrough
22	Auxiliary device support
23	Auxiliary device support (polling device, e.g. Bosch Spreader, Dickey John Salt Spreader)
24	Auxiliary device support (non-polling device, e.g. Parker Spreader)

Notes:

- default is **cmd mode 2 0 0**
- ttyAM2 is used for STM communication.
  To escape out of the mode (to get a command prompt ? console) do the following:
  - **mode = 3** ? type EXIT, type **cmd port n bbbb** (where n is the serial port number and bbbb is the current baud rate)
  - **mode = 4** ? type +++, wait 3 seconds, type **cmd port n bbbb** (where n is the port number and bbbb is the current baud rate); Refer to [pad esc] and [pad esct] for escape sequence

Examples:

1. Set primary serial port to use PAD :
   cmd mode 4 0 0
1. Set primary serial port to use Console, and secondary serial port to use PPP :
   cmd mode 2 3 0
1. Set primary serial port to use Console, and secondary serial port to use client mode connection for external Garmin communications :
   cmd mode 2 18 0

See also: [Serial Port Settings], [MODBUS], [PAD], [RFID Card Reader Support], [Garmin PND]

modemid <*string*>

Assigns a user configurable ID to the CTM-200 gateway containing up to 15 alphanumeric characters.

Notes:

- If no ID is given then the gateway?s 11-digit decimal ESN (CDMA/EV-DO devices only) or 15-digit decimal IMEI (GSM/GPRS/HSPA devices only) will be used if available.
- If less than 15 characters is entered, trailing 0?s will be automatically inserted in [message type 112].

Examples:

1. set the gateway ID to <CAR1234>
   cmd modemid CAR1234

See also: [Cellular]

modemmode *n*

Configures the modem for "half bridge mode"

This command is used to provide the connected device, such as a laptop the same IP address that is assigned to the modem.
This command is useful for application software that requires a specific IP address to operate properly.

n = 0	modem mode off (default)
n = 1	modem mode on

Notes:

- In modem mode, remote web interface, remote ssh/telnet on the modem are not available.
- On the CTM-200, this feature is only supported on the LAN0 Ethernet port
- For a static IP configuration, the client computer's Ethernet settings must be configured to use the WAN IP address, Gateway IP address, and DNS addresses of the phone card/module. If the modem has an active wireless connection, obtain these addresses from output displayed by using [syslog].

Examples:

1. enable modem mode
   cmd modemmode 1

See Also: [Half Bridge]

modemmodedhcp *n*

Configures the modem to use DHCP when configured for "half bridge mode"

n = 0	modem mode will not use DHCP (**default for r2.0.5.3034 and earlier**)
n = 1	modem mode will use DHCP (**default for r2.0.5.3041 and later**)

Notes:

- The client computer's Ethernet settings must be configured to use DHCP to obtain an IP address automatically
- **For r2.0.5.3034 and earlier**: If **modemmodedhcp** is enabled, the client computer mac address must also be configured using **cmd clientmac**

Examples:

1. Use DHCP with modem mode :
   cmd modemmodedhcp 1

See Also: [Half Bridge]

msgredirect add *xxx.xxx.xxx.xxx yyyyy*

Add a redirect target used by the message redirector.

xxx.xxx.xxx.xxx = 0.0.0.0 to 255.255.255.255	redirect target IP address in decimal
yyyyy = 0 to 65535	redirect target port number in decimal

Examples:

1. Add a single redirect target with the specified IP and port :
   cmd msgredirect add 175.181.206.21 18357
2. Add a redirect target to broadcast incoming messages to UDP port 10443 on the entire LAN0 local subnet :
   cmd msgredirect add 192.168.1.255 10443

See also: [Message Redirector]

Firmware revision 2.0.5.2969

msgredirect del *xxx.xxx.xxx.xxx yyyyy*

Delete a redirect target used by the message redirector.

xxx.xxx.xxx.xxx = 0.0.0.0 to 255.255.255.255	redirect target IP address in decimal
yyyyy = 0 to 65535	redirect target port number in decimal

Example:

1. Delete a redirect target to a single target with the specified IP and port :
   cmd msgredirect del 175.181.206.21 18357

See also: [Message Redirector]

Firmware revision 2.0.5.2969

msgredirect enable *n*

Enables/disables the message redirector on the CTM-200. The message redirector redirects incoming UDP packets from a server to another server/remote IP address or to local devices connected to LAN1 or LAN0 of the CTM-200.

n = 0	disable the message redirector (default)
n = 1	enable the message redirector

Example:

1. Enable the message redirector :
   cmd msgredirect enable 1

See also: [Message Redirector]

Firmware Revision 2.0.5.2969

msgredirect list

Display a list of redirect targets configured for the message redirector.

Examples:

1. List currently configured redirect targets :
   cmd msgredirect list

See also: [Message Redirector]

Firmware revision 2.0.5.2969

msgredirect port *xxxxx*

Configure listening port used by the message redirector. Packets arriving on this UDP port will be redirected to configured redirect targets when the message redirector is enabled.

xxxxx = 0 to 65535	message redirector listening port number in decimal

Examples:

1. Configure message redirector listening UDP port :
   cmd msgredirect port 18357

See also: [Message Redirector]

Firmware revision 2.0.5.2969

msgredirect remip *xxx.xxx.xxx.xxx*

Restrict the message redirector to redirect incoming messages originating from a specific remote source IP address.

xxx.xxx.xxx.xxx = 0.0.0.0 to 255.255.255.255	remote source IP address in decimal (default: 0.0.0.0, which does not restrict incoming messages based on remote source IP)

Examples:

1. Redirect incoming messages from the remote source IP address 1.2.3.4 only :
   cmd msgredirect remip 1.2.3.4
1. Redirect incoming messages from any remote source IP address :
   cmd msgredirect remip 0.0.0.0

See also: [Message Redirector]

Firmware revision 2.0.5.2969

multiwan enable *n*

Enable/disable multiwan configuration

n = 0	disable (**default**)
n = 1	enable

Examples:

1. Enable multiwan :
   cmd multiwan enable 1

See also: [multiwan mode]

Firmware revision 2.0.5.3058

multiwan mode *m*

Set multiwan mode type. Multiwan mode types can be used to configure special packet routing configurations.

m = 0	none (**default**)
m = 1	wi-fi traffic on lan0 ethernet, cell traffic on lan1 ethernet
m = 2	wi-fi traffic on lan1 ethernet, cell traffic on lan0 ethernet

Notes:

- multiwan modes 1 or 2 can only be used with a dual-mode cell/wi-fi client configuration (cmd wlan enable 1)
- lan bridging (cmd lanbridge) must not be enabled when using multiwan modes 1 or 2

Examples:

1. Enable multiwan so that all traffic on lan0 port uses wi-fi client interface :
   cmd wlan enable 1
   cmd multiwan enable 1
   cmd multiwan mode 1

See also: [multiwan enable]

Firmware revision 2.0.5.3058

netwd *t n target p m*

Sets the network watchdog feature.
This feature is used to listen for incoming data traffic to make sure there is network connectivity.
If no data is received within the watchdog timer time out period **(t * n)**, the modem will disconnect from the network and reconnect to the network. If the watchdog timer expires a second time after attempting to reconnect unsuccessfully the first time (no data received), the modem will be power cycled.

t = 0	1 = enable , 0 = disable (default = 1)
t = 1 to 65535	time period to ping target (default = 3600 seconds)
n = 0 to 65535	number of failed attempts before disconnecting and reconnecting to the network (default = 1 failed attempt)
target	ping target : IP address or URL (default = 8.8.8.8)
p = 0 to 16	number of pings per test (default = 10). If p = 0, no pings will be sent and network RX/TX traffic will be used to determine network connection.
m = 0 to 65535	max time with no network connection before power cycling (default = 3600 secs). Set m = 0 to disable the max time with no network connection watchdog.

Notes: To ensure normal operation when connected to a private network, the **target** parameter of this command must be configured with an accessible ping target.

Examples:

1. Set the timer to 30 seconds and check 6 times :
   cmd netwd 30 6

   In the above example, the command will ping the target URL/IP address at **30** seconds intervals. If no successful ping responses for **6** consecutive intervals **6 x 30 = 180** sec. the command will disconnect and reconnect to the network. If a reconnect does not resolve the issue, the command will cycle the modem power completely after an additional 6 intervals of unsuccessful ping responses.

1. Set the timer to 30 seconds and check 3 times, and set max no connection time to 5 minutes :
   cmd netwd 30 3 8.8.8.8 5 300
1. Change the ping target to 10.1.2.3 :
   cmd netwd 3600 1 10.1.2.3 10 3600

See also: [Watchdog Timers]

networktime *n*

Set priority of cellular network time as an external system time synchronization source.

n = 0	Disabled
n = 1 to 3	Priority relative to other external system time synchronization sources with 1 = highest (**default = 2**)

Example:

1. Set cellular network time as highest priority relative to other external time synchronization :
   cmd networktime 1

See also: [Time Synchronization]

Firmware revision 1.3.0.1729

nmeamode *n*

Sets the NMEA 0183 version that applies to the GPS message format for GPGLL, GPRMC, and GPVTG sentences. NMEA 0183 v3.0 standard supports an additional field for the Mode Indicator.

n = 0	use NMEA 0183 v2.0 messages (default)
n = 1	use NMEA 0183 v3.0 messages

Examples:

1. Enable NMEA 0183 v3.0 message format :
   cmd nmeamode 1

See also: [GPS Configuration]

ntpserver *url*

Set the network time protocol (NTP) server used by the modem's built-in NTP client for external system time synchronization.

url	the URL/IP address of the NTP server. (**default pool.ntp.org**)

Notes:

- Requires a non-zero priority for [ntptime]

Examples:

1. Use an alternate NTP server :
   cmd ntpserver 0.north-america.pool.ntp.org :

See also: [Time Synchronization]

ntptime *n*

Set priority of the built-in network time protocol (NTP) client as an external system time synchronization source.

n = 0	Disabled
n = 1 to 3	Priority relative to other external system time synchronization sources with 1 = highest (before revision 3098 **default = 3**, after revision 3098 **default = 0**)

Examples:

1. Set NTP time as highest priority relative to other external time synchronization sources :
   cmd ntptime 1

See also: [Time Synchronization]

obdcond *n b t mt [trig1 ... trig4]*

Sets the condition(s) that will trigger an OBD report.

n = 1 to 8	OBD trigger number
b = 0	conditional operator for all following parameters: **Off**
b = 1	conditional operator for all following parameters: **AND**
b = 2	conditional operator for all following parameters: **OR**
t = 0	timeout disabled
t = 1 to 65535	timeout in seconds
t = t or T	timeout disabled, transition is enabled
mt = 0 to 65535	maximum reporting rate in seconds (minimum time between reports)

Optional: **trigx** trigger parameter *x* enclosed in single quotes and without spaces in between, in the form **'pid^val'** where:

pid = p1 to pb	engine parameters as per [OBD2/J1939 Parameters Table] except for **p4** and **id**
^ - >	trigger using greater than operator
^ - =	trigger using equal to operator
^ - <	trigger using less than operator
val	engine parameter value that sets off the trigger, in decimal nnnn.nn (refer to [OBD2/J1939 Parameters Table] for allowable range of values)

Notes:

- To use **obdcond** as a timed trigger ONLY, you must verify that you are receiving valid OBD data (ie. **cmd obddata** cannot return "**ERROR**")

Examples of OBD trigger parameters:

1. trigger is set off when p1 (vehicle speed) is greater than 0 km/h :
   'p1>0'
2. trigger is set off when p2 (engine RPM) is equal to 5000 RPM :
   'p2=5000'
3. trigger is set off when p8 (engine coolant temperature) is less than 200.75°C
   'p8<200.75'

Examples:

1. Set OBD trigger #1 to send a report every **60** seconds :
   cmd obdcond 1 1 60
2. Set OBD trigger #2 to send a report every **30** seconds **AND** P1 (vehicle speed) is equal to **0.0** km/h with a maximum report rate of one every **5** seconds :
   cmd obdcond 2 1 30 5 'p1=0.0'
3. Set OBD trigger #3 to send a report every **60** seconds **OR** P1 (vehicle speed) is greater than **0** km/h **OR** P2 (engine RPM) is greater than **2000** with a maximum report rate of one every **5** seconds :
   cmd obdcond 3 2 60 5 'p1>0' 'p2>2000'
4. Set OBD trigger #4 to send a report **only** when P1 (vehicle speed) is less than **10** km/h AND P2 (engine RPM) is equal to **0** RPM AND P7 (calculated engine load value) is equal to **0** percent AND P8 (engine coolant temperature) is **-40**°C with a maximum report rate of one every **15** seconds :
   cmd obdcond 4 1 0 15 'p1<10.00' 'p2=0.00' 'p7=0.00' 'p8=-40.00'
5. Triggers whenever p5 changes between p5 == 1 to p5 != 1 :
   cmd obdcond 3 2 t 0 'p5=1'

See Also: [OBD2/J1939 Parameters Table], [Engine Diagnostics Support]

obddata

Displays the current OBD engine parameters and corresponding values obtained from the OBDII transmitter and the time since they were last updated.

Notes:

- If no engine parameters have been obtained yet, the command returns **ERROR**
- This command is read-only.

Examples:

1. display OBD engine parameters and time since they were last updated :
   cmd obddata

See Also: [OBD2/J1939 Parameters Table], [Engine Diagnostics Support]

Firmware revision 1.2.0_RC5 (1153)

obdreport *n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for a OBD triggered report.

n = 1 to 8	OBD trigger condition number
r1 to r8 = 1 to 999	report number
r1 to r8 = 1020 to 1027	**(Firmware 3034 and above)** GPS reports 1 to 8
r1 to r8 = 1040 to 1047	**(Firmware 3034 and above**) I/O reports 1 to 8

Examples:

1. Set general report #1, #2 and #4 for OBD triggered report #1 :
   cmd obdreport 1 1 2 4
2. Set I/O report #1 (*1040*) and general report #5 for OBD triggered report #2 :
   cmd obdreport 2 1040 5

See Also: [Engine Diagnostics Support], [General Reports]

obdsp *n*

Sets the protocol used by the OBDII transmitter.

n = 0	Automatic
n = 1	SAE J1850 PWM
n = 2	SAE J1850 VPW
n = 3	ISO 9141-2
n = 4	ISO 14230-4 KWP (slow)
n = 5	ISO 14230-4 KWP (fast)
n = 6	ISO 15765-4 CAN (11 bit ID, 500 Kbaud)
n = 7	ISO 15765-4 CAN (29 bit ID, 500 Kbaud)
n = 8	ISO 15765-4 CAN (11 bit ID, 250 Kbaud)
n = 9	ISO 15765-4 CAN (29 bit ID, 250 Kbaud)
n = 10	SAE J1939 CAN (29 bit ID, 250 Kbaud)
n = 11	USER1 CAN (11 bit ID, 125 Kbaud)
n = 12	USER2 CAN (11 bit ID, 50 Kbaud)

Notes:

- Option 0 (Automatic) only replaces OBD2 protocol options 1-9. Some vehicles may exhibit problems with automatic protocol discovery. **obdsp** must specifically be set to match the protocol on those vehicles.

Examples:

1. Set the OBDII transmitter to use the J1939 protocol :
   cmd obdsp 10

See Also: [OBD2/J1939 Parameters Table], [Engine Diagnostics Support]

Firmware revision 1.2.0_RC7(rev.1187)

odometer *n*

Sets/queries the odometer.
The odometer keeps track of the distance travelled in km by using GPS (**cmd can odometer 0**) (**Default**), OBD (**cmd can odometer 1**) or both (**cmd can odometer 2**)

n = 0	Odometer reset to 0
n = 1 to 1999999	Odometer value

Notes:

- The odometer will roll over to 0 km when the current odometer value exceeds the maximum.

Examples:

1. Reset the GPS odometer value to 0 :
   cmd ctm15x'
   cmd odometer 0
1. Set the GPS odometer to 100000 km :
   cmd ctm15x
   cmd odometer 100000

See also: [Engine Diagnostics Support], [GPS Configuration]

orientation *n*

Set device mounting orientation within the vehicle when using the accelerometer.

Orientation Code	Description	Vector for hard acceleration	Vector for hard turning
n = 0	Not specified (**default**)		
n = 1	LEDs pointing up and located towards the front of the vehicle	Y	X
n = 2	LEDs pointing up and located towards the passenger side	-X	Y
n = 3	LEDs pointing up and located towards the rear of the vehicle	-Y	-X
n = 4	LEDs pointing up and located towards the driver side	X	-Y
n = 5	LEDs pointing down and located towards the front of the vehicle	Y	-X
n = 6	LEDs pointing down and located towards the passenger side	X	Y
n = 7	LEDs pointing down and located towards the rear of the vehicle	-Y	X
n = 8	LEDs pointing down and located towards the driver side	-X	-Y
n = 9	GPIO connector pointing up and located towards the front of the vehicle	Y	-Z
n = 10	GPIO connector pointing up and located towards the passenger side	Z	Y
n = 11	GPIO connector pointing up and located towards the rear of the vehicle	-Y	Z
n = 12	GPIO connector pointing up and located towards the driver side	-Z	-Y
n = 13	GPIO connector pointing down and located towards the front of the vehicle	Y	Z
n = 14	GPIO connector pointing down and located towards the passenger side	-Z	Y
n = 15	GPIO connector pointing down and located towards the rear of the vehicle	-Y	-Z
n = 16	GPIO connector pointing down and located towards the driver side	Z	-Y
n = 17	Standing on a short edge away from GPIO connector which is located towards the front of the vehicle	X	Z
n = 18	Standing on a short edge away from GPIO connector which is located towards the passenger side	-Z	X

n = 19	Standing on a short edge away from GPIO connector which is located towards the rear of the vehicle	-X	-Z
n = 20	Standing on a short edge away from GPIO connector which is located towards the driver side	Z	-X
n = 21	Standing on a short edge closer to GPIO connector which is located towards the front of the vehicle	X	-Z
n = 22	Standing on a short edge closer to GPIO connector which is located towards the passenger side	Z	X
n = 23	Standing on a short edge closer to GPIO connector which is located towards the rear of the vehicle	-X	Z
n = 24	Standing on a short edge closer to GPIO connector which is located towards the driver side	-Z	-X

See Also: [Accelerometer]

Firmware revision 2.0.3.2255-80

otasp

This command is used to perform automatic wireless network activation and updates any required network related files that are embedded in the wireless modem.

The modem responds with one or more of the following messages:

- SPL Unlocked
- Authentication key has been exchanged
- Shared secrets data has been updated
- New NAM parameters have been downloaded
- New MDM has been downloaded
- IMSI has been downloaded
- PRL has been downloaded

Notes:

- During updating, if any of the above data is unsuccessful, an OTASP Timeout message will be displayed.
- A progress message OTASP Processing will be displayed every 10 seconds.
- When the OTASP process has been completed, the OTASP Disconnected message will be displayed.

Examples:

1. Initiate automatic wireless network activation :
   cmd otasp

See Also: [Cellular]

pad

List all PAD configuration commands.

Notes:

- On CTM devices that support multiple serial ports the second PAD configuration commands can be viewed by entering **cmd pad2**.

Examples:

1. list PAD configuration commands :
   cmd pad
2. list second serial port PAD configuration commands :
   cmd pad2

See also: [PAD]

pad clientport port

Sets the default client PAD port number for use with dialup emulation

port = 0 to 65535	dialup emulation PAD client port number. **(Default 5006)**

Notes:

- this command is valid for only **cmd pad mode 6** or **cmd pad mode 7** when the dial command **ATDT** is issued by an external serial device to initiate an outgoing connection.

Examples:

1. Set the dialup emulation PAD client port to 4444 :
   cmd pad clientport 4444

See also: [PAD]

---

pad echo *n*

Sets the PAD echo mode ? if echo is enabled then all data sent to the modem on its RS232 port by an external device is echoed back to that device.

n = 0	PAD echo mode: disabled
n = 1	PAD echo mode: enabled (**default**)

Examples:

1. Disable the PAD echo ? characters received on the modem?s RS232 port will not be echoed to the connected device :
   cmd pad echo 0

See also: [PAD]

Firmware revision 1.2.0_RC6(rev.1170)
Firmware revision 2.0.0.2126

pad esc *str*

Sets the PAD escape sequence used to return to command line mode.

str	PAD escape sequence, 10 characters maximum, no spaces, case sensitive Default is **+++**

Notes:

- When using the escape sequence it is necessary to wait the guard time ([pad esct]) before entering data
- Enter only the escape sequence ,do not enter any other characters (ie. do not press "Enter" after the escape sequence is entered)

Examples:

1. Set the PAD escape sequence to ASCII string 12345 :
   cmd pad esc 12345

See also: [PAD]

Firmware revision 1.2.0_RC6(rev.1170)
Firmware revision 2.0.0.2126

pad esct *n*

Sets the PAD escape guard time.
This is the idle time before and after the PAD escape sequence which must be present for the escape sequence to be recognized.

n = 0 to 65535	PAD escape guard time in seconds (**Default 3**)

Notes:

- values greater than **8 seconds** shouldn't be used in **TCP PAD client mode**.

Examples:

1. Set the PAD escape guard time to 4 seconds :
   cmd pad esct 4

See also: [PAD]

Firmware revision 1.2.0_RC6(rev.1170)
Firmware revision 2.0.0.2126

pad fifo *n*

Sets the internal communication mechanism used by PAD.

n = 0	Use a serial port directly for PAD communication (**default**)
n = 1	Use FIFO RX/TX files instead of a serial port. Should be used with Garmin mode - server only, **cmd mode 19**

Examples:

1. Enable PAD FIFO communication mechanism for Garmin mode - server only, **cmd mode 19**:
   cmd pad fifo 1

See also: [PAD]

Firmware revision 2.0.4.2591

pad fwdc *x r*

Sets the PAD forwarding character and to remove the forwarding character before forwarding the packet (optional). Default forwarding character = 13 (ASCII <enter>), default forwarding character removal disabled.

x = 0	**pad fwdt** or **pad fwdl** will invoke sending the packet
x = 1 to 255	PAD forwarding character representing an ASCII character (**default 13**)
r = 0	Do not remove the forwarding character before forwarding the packet (**default**)
r = 1	Remove the forwarding character before forwarding the packet

---

Examples:

1. Sets the PAD forwarding character to ASCII <space> and do not remove the forwarding character before forwarding the packet :
   cmd pad fwdc 32 0
1. Sets the PAD forwarding character to ASCII <space> and remove the forwarding character before forwarding the packet :
   cmd pad fwdc 32 1

See also: [PAD]

FIrmware revision 1.3.1.1939
Firmware revision 2.0.0.2126

pad fwdl *x*

x = 0	send every characters immediately
x = 1 to 1000	maximum PAD packet length (**default 40**)

Examples:

1. Configure the received RS232 data to be sent in packets of 10 characters each :
   cmd pad fwdl 10

See also: [PAD]

Firmware revision 1.2.0_RC6(rev.1170)
Firmware revision 2.0.0.2126

pad fwdt *t*

t = 0	Disable forwarding timer. Every character will be sent immediately
t = 1 to 255	PAD forwarding time in increments of 50ms (**default 1**)

Examples:

1. Set the PAD forwarding time to 2 seconds :
   cmd pad fwdt 40

See also: [PAD]

Firmware revision 1.2.0_RC6(rev.1170)
Firmware revision 2.0.0.2126

pad ip *ipaddr*

Sets the remote PAD IP address.

ipaddr = 0.0.0.0 to 255.255.255.255	remote IP address. (**Default 0.0.0.0**)

Notes:

- Use **0.0.0.0** to set the modem in PAD server mode.

Examples:

1. Set the PAD IP address to 192.168.1.1 :
   cmd pad ip 192.168.1.1

See also: [PAD]

Firmware revision 1.2.0_RC6(rev.1170)
Firmware revision 2.0.0.2126

pad mode *x*

Sets the PAD mode.

x = 0	start up UDP PAD mode. The modem will revert to server mode once the connection is closed. (**default**)
x = 1	start up TCP PAD mode. The modem will revert to server mode once the connection is closed.
x = 2	start up UDP PAD client mode - one session. The modem will revert to command mode once the connection is closed.
x = 3	start up TCP PAD client mode - one session. The modem will revert to command mode once the connection is closed.
x = 4	start up persistent UDP PAD client mode
x = 5	start up persistent TCP PAD client mode
x = 6	start up Dialup Emulation over UDP mode
x = 7	start up Dialup Emulation over TCP mode
x = 8	start up PAD with the file based reporting system
x = 9	start up hybrid PAD mode (UDP)
x = 10	start up hybrid PAD mode (TCP)

Notes:

- The connection is closed if one of the following occurs:
  - **pad svct** idle timeout expires
  - **pad svct** maximum session timeout expires
  - **cmd pad reset** is executed
  - The connection is closed by remote host (TCP PAD only)
- If [pad ip] is set to 0.0.0.0, PAD will start in server mode. Otherwise it will start in client mode. Note that for the client modes (2, 3, 4 and 5), [pad ip] must be different than 0.0.0.0. Note that for dialup emulation modes (6 and 7), [pad clientport] must be set.

Examples:

1. Set to TCP PAD mode :
   cmd pad mode 1

See also: [PAD]

Firmware revision 1.2.0_RC7(rev.1187)
Firmware revision 2.0.0.2126

pad pfc *x*

Sets the PAD postfix character that is added at the end of each packet

x = none	Disabled (**default**). No character is added to the end of a PAD packet.
x = 1 to 255	PAD forwarding character representing an ASCII character.

Examples:

1. Set the PAD postfix character to ASCII <LF> :
   cmd pad pfc 10

See also: [PAD]

Firmware revision 1.3.1.1939
Firmware revision 2.0.1.2225

pad port *p*

Sets the remote PAD port number.
This is the listening port if the modem is in PAD server mode.

p = 0 to 65535	remote PAD port number. (**default 5005**).

Examples:

1. Set the PAD port to 5005 :
   cmd pad port 5005

See also: [PAD]

Firmware revision 1.2.0_RC6(rev.1170)
Firmware revision 2.0.0.2126

pad reset

Resets the PAD connection.

Notes:

- The actions taken by this command are to drop the PAD connection and to return the modem to server mode.
- These actions are equivalent to those that occur when the [pad svct] timer expires.

Examples:

1. Reset the PAD port :
   cmd pad reset

See also: [PAD]

Firmware revision 1.2.0_RC6(rev.1170).
Firmware revision 2.0.0.2126

pad secure *n*

Secure access to the modem's PAD server from the Internet.
If enabled, it will not be possible to remotely access the PAD server via the port specified in [pad port] and using the current IP address allocated to the CTM-200 by the network.
This is to support applications where the servers may be accessed through SSH tunneling.

n = 0	allow direct access to PAD server from Internet (**default**)
n = 1	secure - do not allow direct access to PAD server from Internet

Examples:

1. Set the CTM-200 to secure access to PAD server from Internet :
   cmd pad secure 1

See also: [PAD]

Firmware revision 1.3.0.2090

pad svct *n [c]*

Sets the PAD server connection timeout.
If no data is sent or received within this timeout value, the PAD connection will be dropped and the modem will return to server mode.
If the optional parameter for the maximum PAD connection timer is specified, once the timer expires, the current PAD connection will be dropped regardless of the data connection condition.
The modem will revert to the current PAD mode setting and maintain the PAD session.

n = 0	PAD server connection timeout: disabled
n = 1 to 65535	PAD server connection timeout in seconds (**default 15**)
c = 0	Maximum PAD connection time: disabled (**default**)
c = 1 to 65535	Maximum PAD connection time in seconds

Examples:

1. Configure the CTM-200 to revert to server mode after 10 seconds of data inactivity :
   cmd pad svct 10
1. Configure the PAD connection to be dropped after 60 seconds :
   cmd pad svct 15 60

See also: [PAD]

Firmware revision 1.2.0_RC6(rev.1170)
Firmware revision 2.0.0.2126

panicreportack *t*

This command will set the modem to wait for a Pendant panic triggered report (PANIC or MPANIC message only) and send the corresponding acknowledgment message.

t = 0	Disables panicreportack (**Default**)
t = 1 to 65535	Time period in seconds to wait for the next PANIC or MPANIC message from a Pendant and send it an ACK

Notes:

- For this command to function, the modem must be configured with **cmd wpan acktype s** set.
- When this command is set, **panicreport** will be disabled to stop triggering the script.
- This command is meant to be used with custom report triggered scripts via **reportscripts**.
- This command is volatile.
- When **panicreportack** is entered without parameters, the command returns the configured time period and the elapsed time, in seconds, since **panicreportack** was set.

Examples:

1. Wait for 60 seconds for a PANIC or MPANIC message and send a Pendant an ACK if received :
   cmd panicreportack 60

   Query the time period set for waiting for a PANIC or MPANIC message to ACK, and the current time elapsed since **panicreportack** was set :

```
cmd panicreportack
cmd panicreportack 60 15
```

See also: [Down Pendant], [General Reports]

Firmware revision 1.3.0.1731

panicreport *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command will set the report(s) to be used for pendant triggered panic reports (PANIC and MPANIC only)

r = 0	Disables the report (**default**)
r = 1 to 999	Report number

Notes:

- this command requires the modem to be listening for traffic from the WPAN gateway, this requires **cmd mode 10** to be configured if using external WPAN gateway
- this command does not support server ACK mode and [reptype] 8 and 9
- Panic report is triggered by a panic message received from the Pendant. The following message is appended to the report:

$PPEN,ID,SEQ,MES*CHKSUM
ID - 64 bit unique hex ID of Pendant
SEQ - Packet sequence number
MES - Pendant panic message payload (PANIC or MPANIC)
CHKSUM - NMEA message checksum

Example:

```
$PPEN,0013A200402CB498,17,PANIC*07
```

Examples:

1. Use report 1 for pendant panic triggered reports :
   cmd panicreport 1

See also: [Down Pendant], [General Reports]

Firmware revision 1.3.0.1727

panicreportack t

This command will set the modem to wait for a Pendant panic triggered report (PANIC or MPANIC message only) and send the corresponding acknowledgment message.

t = 0 disables **panicreportack** (default)
t = 1 to 65535 time period, in seconds, to wait for the next PANIC or MPANIC message from a Pendant and send it an ACK

For **panicreportack** to function properly, the modem must be configured with [set to server type acknowledgment and with [panicreport]. When **panicreportack** is set, [will be disabled to stop triggering the script. This command is meant to be used with custom report triggered scripts via [reportscripts] and is always volatile.

When **panicreportack** is entered without parameters, the command returns the configured time period and the elapsed time, in seconds, since **panicreportack** was set.

Examples:

1. Wait for 60 seconds for a PANIC or MPANIC message and send a Pendant an ACK if received

```
cmd panicreportack 60
OK
```

Query the time period set for waiting for a PANIC or MPANIC message to ACK, and the current time elapsed since **panicreportack** was set

```
cmd panicreportack
cmd panicreportack 60 15
OK
```

See also: [[panicreport] [[wpanacktype]

Command operation has been verified in R1.3.0.1731

panicreptype *m*

This command will set whether panicreport will generate ASCII/NMEA message (e.g. `$PPEN,0013A200402CB498,17,PANIC*07`) or binary/ULCP message ([msg 93]).

m = 0	ASCII (**Default**)
m = 1	Binary

Examples:

1. Set panicreport to generate binary messages :
   cmd panicreptype 1

See also: [Down Pendant], [General Reports]

Firmware revision 2.0.5.3257

pendantreport *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the general report(s) to be used for pendant triggered reports. Pendant reports are triggered by any message received from the Pendant including ON and OFF messages.

Up to 8 reports can be assigned to the pendantreport.

r = 0	Disables the report (**Default**)
r = 1 to 999	Report number

Notes:

- this command requires the modem to be listening for traffic from the WPAN gateway, this requires **cmd mode 10** to be configured if using external WPAN gateway
- Pendant report is triggered by any message received from the Pendant. The following message is appended to the report:

$PPEN,ID,SEQ,MES*CHKSUM
ID - 64 bit unique hex ID of Pendant
SEQ - Packet sequence number
MES - Pendant message payload
CHKSUM - NMEA message checksum

Example:

```
$PPEN,0013A200402CB498,17,PANIC*07
```

Examples:

1. Use report 1 for pendant triggered reports :
   cmd pendantreport 1

See also: [Down Pendant], [General Reports]

The format of this command has changed from R1.2.0 to R1.2.1. R1.2.0 allowed a single report, whereas up to 8 reports can now be configured.

pin *n*

Sets the 4-digit PIN code to lock the SIM card used with cell devices. A 4-digit PIN code is required outside of North America for EDGE/GSM/HSPA device activation.

n = 0	clear PIN code
n = 0001 to 9999	set 4-digit PIN code to lock SIM card

Notes:

- By default a PIN code is not set.

Examples:

1. set the PIN code to 1234
   cmd pin 1234

See also: [Cellular]

ping *n iii.iii.iii.iii*|*website*

Configures the modem to ping a specific IP address or website periodically.

n = 0	Disables ping (**default**)
n = 1 to 65535	number of seconds between pings
iii.iii.iii.iii	IP address of the site to ping, IP Address must be in the range 0 to 255 for each value of **iii**. If values outside this range are entered, it will be interpreted as a URL (**default 0.0.0.0**)
website name	website to ping

Examples:

1. ping www.google.ca every 10 seconds :
   cmd ping 10 www.google.ca
1. ping 66.102.7.147 every 15 seconds :
   cmd ping 15 66.102.7.147

See also: [Watchdog Timers]

pobd*x n1 [n2] [n3] [n4] [n5] [n6] [n7] [n8]*

Configures the engine - vehicle diagnostic report messages. See [Report Messages] 119 to 126.

x	a, b, c, d, e, f, g, h
n1 to n8	engine parameters as per [OBD2/J1939 table]

Examples:

1. report vehicle speed :
   cmd pobda p1
1. reports engine speed, intake air temperature and total engine hours :
   cmd pobdb p2 p12 p25
1. reports calculated peak acceleration and calculated peak deceleration :
   cmd pobdc pa pb

See also: [Engine Diagnostics Support]

port *n r d p s f*

Configures the baud rate and data format of the specified serial port.

n = 1	configure Primary DB9 port
n = 2	configure Secondary DB9 port
n = 3	configure RS485 port
r = 1200	1200 Baud
r = 2400	2400 Baud
r = 4800	4800 Baud
r = 9600	9600 Baud
r = 19200	19200 Baud
r = 38400	8400 Baud
r = 57600	57600 Baud
r = 115200	115200 Baud (**default**)
d = 5,6,7 or 8	number of data bits (**default 8**)
p = n or N	no parity (**default**)
p = e or E	even parity
p = o or O	odd parity
s = 1 or 2	number of stop bits (**default 1**)
f = 0	no flow control (**default**)
f = 1	software flow control
f = 2	hardware flow control

Notes:

- For MODBUS Serial Master Gateway there are 2 options only for the data bit configuration:
  - 7 and 8 for ASCII Mode.
  - 8 for RTU-over-UDP Mode.

Examples:

1. configure primary serial port with baud rate=115200bps, 8 data bits, no parity, 1 stop bit and hardware flow control :
   cmd port 1 115200 8 n 1 2

See also: [Serial Port Settings]

ppp

Provide the connected device a PPP connection through the serial port.

Notes:

- To escape from this mode and return to the command line, type **EXIT** in the terminal program.
- When the modem is configured for PPP mode, the IP addresses used in the serial PPP connection will use the same subnet as the modem's Ethernet LAN IP, after configuring using [lanip]. For example, if the modem was configured with a LAN IP of 192.168.6.1, the serial PPP connection will use 192.168.6.200 and 192.168.6.202 as the IP addresses for the serial PPP client and the modem, respectively.
- When using **cmd ppp**, the modem's DHCP server IP pool, configured using [landhcp], must not include the range x.x.x.200 - x.x.x.202.

Examples:

1. Start the modem into PPP mode:
   cmd ppp

See also: [Serial Port Settings]

- Before firmware revision 1.3.0.1779: Dial string for EVDO modems is **#777** and the dial string for HSPA modems is ***99*1#**
- After firmware revision 1.3.0.1779: Dial string of **#777** is used for all serial PPP connections

pswd *n*

Sets the password used for wireless network access via simple IP. This is often set to the electronic serial number (ESN) of the modem.

n	a maximum of 40-character alpha-numeric characters

Examples:

1. set the password to 12345678900 :
   cmd pswd 12345678900

See Also: [Cellular]

pupcond *n a*

Sets the condition(s) that would trigger a power up report.

n = 1 to 8	power up condition numbers
a = 0	power up trigger disabled (**default**)
a = 1	power up trigger enabled

Examples:

1. enable powerup condition 1 :
   cmd pupcond 1 1
1. disables powerup condition 2 :
   cmd pupcond 2 0

See Also: [Power-up Reports], [General Reports]

pupreport ***n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]***

This command sets the report(s) to be used for power-up triggered reports.

n = 1 to 8	power-up trigger condition
r1 to r8 = 1 to 999	report number

Notes:

- When sending power up reports locally/remotely, power up reports will be stored on the CTM-200 until a signal is obtained. For the stored reports to be sent, the following conditions must be met:
  - the CTM-200 must obtain a signal
  - **(Only applies to firmware below 3041)** The same report number(s)**(r1 to r8)** used in cmd pupreport must be used in another command (ie obdreport, vccreport)
  - **(Only applies to firmware below 3041)** The 'other' command (ie. [obdreport], [vccreport]) must be sending live data

---

Examples:

1. Configure reports #2 and #999 for power-up trigger condition #1 :
   cmd pupreport 1 2 999

See also: [Power-up Reports]

pwr accelt *a*

Configure the CTM-200's wake up condition for acceleration based on internal accelerometer.

a = 0	Disabled (**default**)
a = 1 to 8000	acceleration threshold in mg

Examples:

1. configure to wake the gateway when there is acceleration of 1.5g :
   cmd pwr accelt 1500

See also: [Power Management]

Firmware revision 2.0.1.2221

pwr geofence *lat lon rad mode*

Configure the CTM-200 gateway to wake up based on a geofence.

lat	center point latitude in deg (-90.0 - 90.0) (**default 0**)
lon	center point longitude in deg (-180.0 - 180.0) (**default 0**)
rad = 0	Disabled (**default**)
rad = 1 to 65535	boundary radius (m)
mode = 0	Wake up once the fence is exited (**default**)
mode = 1	Wake up once the fence is entered
mode = 2	Wake up once the fence is entered or exited (crossed)

Notes:

- If the wake event is TRUE when the gateway enters minimum power mode, it needs to reach a FALSE state and then TRUE again before waking the gateway.
  - For example, if **cmd pwr geofence 49.256548 -122.996718 500 0** is set, then the gateway needs to be outside the 500m radius first and then within the radius to trigger it to wake.

Examples:

1. Wake the gateway if it is moved more than 500m away from the specified location :
   cmd pwr geofence 49.256548 -122.996718 500 0
1. Wake the gateway if it is within 1km of the specified location :
   cmd pwr geofence 49.256548 -122.996718 1000 1
1. Wake the gateway if it crosses the 1500m radius boundary of the specified location :
   cmd pwr geofence 49.256548 -122.996718 1500 2

See also: [Power Management]

Available in firmware revision 2.0.1.2221 and later

pwr mode *n*

Controls the CTM-200?s power mode.

n = 1	puts the gateway in standby mode
n = 2	will power cycle the gateway immediately

Notes:

- **cmd pwr mode 1** will output **ERROR** if a valid [pwr woe] command has not been set.
- If using SMS commands to control/configure the CTM-200, cmd pwr mode 2 should only be issued via SMS on devices running r2.0.4.2540 or later.

Example:

1. power cycle the CTM-200 gateway :
   cmd pwr mode 2
2. place CTM-200 into standby mode :
   cmd pwr mode 1

See also: [General]

pwr override m

Configure the CTM-200 gateway to prevent entering minimum power mode for the current session.
m = 0 : gateway can enter minimum power mode (default)
m = 1 : Prevent gateway from entering minimum power mode

Default: cmd pwr override 0

Example:

Prevent the modem from entering minimum power mode (e.g. while configuring **pwr woe**)

```
cmd pwr override 1
```

Note: This command defaults back to 0 after any and all power-cycles.

The operation of this command has been verified in 2.0.1.2221

pwr rtc *u m*

Configure the CTM-200's wake up condition based on RTC time.

u	UTC time of first wakeup (**default 0**)
m	wakeup period in seconds
m = 0	Wake up on **u** only (once) (**default**)

Examples:

1. Wake up gateway every 1 hr on the hour :
   cmd pwr rtc 0 3600
1. Wake up gateway only once a day :
   cmd pwr rtc 0 86400
1. Wake up gateway at a specific date & time (e.g. New Year's Eve at Sat, 31 Dec 2011 23:59:59 GMT) :
   cmd pwr rtc 1325375999 0
1. To wake up at a specific date & time and then periodically afterwards if gateway is in minimum power mode (e.g. New Year's Eve at Sat, 31 Dec 2011 23:59:59 GMT and then every 10 minutes if gateway is in minimum power mode) :
   cmd pwr rtc 1325375999 600

See also: [Power Management]

Firmware revision 2.0.1.2221

pwr sdwn *a ddddd*

Places the CTM-200 gateway into shutdown mode or minimum power mode (blinking power LED) based on the state of the gateway's standby signal (ignition).

a = 0	disables the standby signal (ignition) event qualifier
a = 1	enables the standby signal (ignition) event qualifier (**default**)
ddddd = 10 to 65535	time in seconds for the standby signal (ignition) to be off for CTM to enter shutdown mode (**default 10**)

Notes:

- The ignition state is controlled by the "white" wire of the 3 wire power connection to the gateway.
- To disable any ignition sense capability connect the "white" wire to the + Voltage "Red" wire.

Examples:

1. Force the gateway to enter minimum power mode when the ignition has been inactive for 1 hr. The gateway will power back up when ignition has been turned on.
   cmd pwr sdwn 1 3600

See also: [Power Management]

Firmware revision 1.2.0_RC7(rev.1187)

pwr speedth *s t*

Configure the CTM-200's wake up condition based on GPS speed.

s = 0 to 254	speed threshold in kph (**default 0**)
t	time in seconds that speed has to be greater than or equal to **s** (**default 0**)

Examples:

1. Force the gateway to wake when GPS speed is greater than 79km/h for more than 30 seconds :
   cmd pwr speedth 80 30

See also: [Power Management]

Firmware revision 2.0.1.2221

pwr temp *l h m*

Configure the CTM-200's wake up condition for temperature.

l	Low threshold in degrees Celsius (-40 to 85) (**default 0**)
h	High threshold in degrees Celsius (-40 to 85) (**default 0**)
m	mode
m=0	Wake up on LOW to HIGH transition (**default**)
m=1	Wake up on HIGH to LOW transition
m=2	Wake up on any transition

Notes:

If the temperature at the time the gateway goes into minimum power mode results in TRUE, the gateway will wait for it to become FALSE before waking up on TRUE.

- For example, if **cmd pwr temp 10 30 1** is set, and if the temperature is lower than 30 degrees Celsius at the time the gateway goes into minimum power mode, the gateway will wait for it to go above 30 degrees Celsius first and will wake up next time it goes below 10 degrees Celsius.

Examples:

1. Wake up when the gateway transitions from above 30 degrees Celsius to under 10 degrees Celsius :
   cmd pwr temp 10 30 1
1. Wake up when the gateway crosses 15 degrees Celsius (e.g. from >15 to <15, or vice versa) :
   cmd pwr temp 15 15 2

See also: [Power Management]

Firmware revision 2.0.1.2221

pwr vcct *vv.v t*

Controls the supply voltage below which the CTM-200 gateway will automatically go into standby mode.

vv.v = 6.0 to 25.5	threshold supply voltage at which the gateway will go into shutdown (**default 9.0**, typical for 12V battery operation)
t = 10 to 255	duration of time in seconds that the supply voltage is below the threshold voltage before gateway enters shutdown (**default 10**)

Examples:

1. Set the threshold to 20.0 volts with 10 seconds delay ? this may be appropriate for a 24 volt battery :
   cmd pwr vcct 20.0 10

See also: [Power Management]

Firmware revision 2.0.1.2221

pwr woe *m t1 t2 t3 f*

Configures what event will wake up the CTM-200 gateway (see list of wake up events below) and how long the gateway will stay awake after the event. This is used to have the gateway in minimum power mode (< 2 mA) until it is required to communicate over the wireless network.

If it is required to have the gateway start its shutdown mode immediately (without waiting for timer **t1** to expire), than use the [pwr mode] command to put the gateway into shutdown with immediate effect.

This command can also be used to configure scheduled power cycles without having to put the gateway into shutdown.

m = 0	disables the power wake on event operation (**default**)
m = 1	enables the power wake on event operation
t1 = 0	disables the ON timer while ignition is OFF (stay on forever ? [pwr sdwn] can be enabled to shutdown the gateway) (**default**)
t1 = 1 to 65535	the ON time while ignition is OFF in minutes (the gateway will remain on for this time after ignition OFF is detected)
t2 = 0	disables the ON timer while ignition is ON or disabled (stay on forever) (**default**)
t2 = 1 to 65535	the ON time while ignition is ON in minutes (the gateway will remain on for this time while ignition is detected ON or is disabled)
t3 = 0	disables the OFF timer - stay in shutdown mode forever or until an input alarm event (or standby signal if enabled in [pwr sdwn]) occurs
t3 = 1 to 1092	the OFF time in minutes - the time that the gateway will stay in shutdown if an input alarm event (or standby signal if enabled in [pwr sdwn]) does not occur (**default 10**)
t3 = c	power cycle the gateway instead of going into minimum power mode
f = 0	disables the input event trigger (**default**)
f > 0	Bit mapped wake up events in hex as described (see 'Value' column below)

Wake Up Events
The following table lists all wake up events and corresponding configuration commands:

bit	Value	Description	Configuration Command
1	00000002	Wake on ignition	[pwr sdwn]
2	00000004	Wake on input 1	[insetup]
3	00000008	Wake on input 2	[insetup]
4	00000010	Wake on input 3	[insetup]
5	00000020	Wake on input 4	[insetup]
6	00000040	Wake on input 5	[insetup]
7	00000080	Wake on input 6	[insetup]
8	00000100	Wake on VCC	[pwr vcct]
9	00000200	Wake on temperature	[pwr temp]
10	00000400	Wake on accelerometer	[pwr accelt]
11	00000800	Wake on GPS	[pwr geofence]
12	00001000	Wake on timer	[pwr woe]
13	00002000	Wake on RTC	[pwr rtc]
14	00004000	Wake on GPS Speed	[pwr speedth]

15	00008000	Wake on Man Down Pendant	[wpan stm 1]
16	00010000	Wake on input 7	[insetup]
17	00020000	Wake on input 8	[insetup]

Notes:

- Each enabled **f** bit will cause the application to configure the corresponding wake up event before going into minimum power mode
- ON timer while ignition ON runs always
- ON timer while ignition OFF runs only when ignition is OFF
- ON timer while ignition OFF gets reset every time ignition is detected as ON
- CTM takes the longest time of ON timer while ignition OFF or **pwr sdwn** to determine when to enter shutdown mode
- Wake up events can be combined by taking the hexadecimal sum of their values.
- By default, the conditional operator for all configured wake up events is OR.
- To configure the conditional operator for all configured wake up events as AND, add hexadecimal 80000000 (**Important note:** When using the AND conditional operator, the corresponding wake up events must be properly configured to ensure the gateway wakes up from minimum power mode.)

Examples:

1. Configure the CTM-200 gateway to power cycle every 12 hours :
   cmd pwr woe 1 0 720 c 0
1. Stay ON while ignition is ON and cycle 10 min ON, 50 min OFF while ignition is OFF :
   cmd pwr woe 1 10 0 50 2
   cmd pwr sdwn 1 10
1. Wake up every day at 9 AM and stay ON for 30 min, with the first wake up starting on February 01, 2011 9:00 AM :
   cmd pwr woe 1 30 0 0 2000
   cmd pwr rtc 1296579600 86400
1. Wake up if moved more than 500 m away from the specified location or every 6 hours while ignition is OFF. Stay on for 10 min. Stay ON while ignition is ON :
   cmd pwr woe 1 10 0 360 802
   cmd pwr geofence 49.256548 -122.996718 500 0
1. Power cycle every 12 hours while ignition is ON. Stay OFF while ignition is OFF :
   cmd pwr woe 1 0 720 c 0
1. Power up when a PANIC/MPANIC/FPANIC message is received from Man Down Pendants :
   cmd pwr woe 1 0 0 0 8000

See also: [Power Management]

Firmware revision 2.0.1.2138

ratesel *n*

Sets the required network rate mode (CDMA vs. EV-DO) of the device. This command is not valid for GSM/GPRS/HSPA devices.

n = 0	1xRTT only
n = 1	EV-DO only
n = 2	Auto Rate Select (hybrid mode) - default

Notes:

- Prior to using the this command, verify that the modem is in manual connection **'cmd mode 1**'.
- Entering **cmd ratesel** without parameters will return an ?ERROR?, this is normal operation.
- this command is valid for Sierra Wireless CDMA/EV-DO data devices and modules only
- The Sierra Wireless AC580 (EV-DO revision 0, Cardbus device) only supports **cmd ratesel 2**

Examples:

1. Set the network rate mode to 1xRTT only
   cmd ratesel 0

See also: [Cellular]

ratetmr *n*

Sets the required network rate test timer of the device. This is used to configure the modem to test for an available EV-DO network while it is in a 1xRTT connection.
This command is valid for Sierra Wireless CDMA/EV-DO data devices and modules only.

n = 0	disable the timer (default)
n = 1 to 65535	time in seconds. Note that time in second is an approximate value; the time between periods will be greater than the ?n? value set

---

Examples:

1. During a 1xRTT connection the modem will disconnect approx. every 120 seconds and then reconnect on the EV-DO network if available, otherwise it will reconnect on the 1xRTT network :
   cmd ratetmr 120

See also: [Cellular]

repaddmes *n x [x2][x3][x4]*

Adds a message type to a report.

n = 1 to 999	report number
x1 to x4	message type to be added, valid message types must be used - [see message list]

Notes:

- Binary messages MUST be placed before ASCII messages. Ex. **cmd repaddmes 1 85 114** = correct, **cmd repaddmes 1 114 85** = incorrect.
- Messages will be sent in a report in the same order that they are added.
- ULCP header messages will be sent as individual UDP packets ? NMEA format messages will be combined into a single UDP packet.

Examples:

1. Add message type #16 ? GPS NMEA GLL ? to report #4 :
   cmd repaddmes 4 16

See Also: [General Reports]

repdelmes *n x*

This command is used to delete a message type (or all messages) from a report.

n = 1 to 999	report number
x	message type to be deleted (0 to delete all messages)

Examples:

1. Delete message type #16 from report #1 :
   cmd repdelmes 1 16
1. Delete all messages from report #4 :
   cmd repdelmes 4 0

See Also: [General Reports]

repemail *n emailaddr*

Sets the email address that the report will be sent to (if configured for email using [reptype]).
The default email address is blank.

n = 1 to 999	report number
emailaddr	email address to which the report will be sent

Notes:

- An email server is required ? see [emailsrv].

Examples:

1. Set the send to email address for report #1 :
   cmd repemail 1 me@?

See Also: [General Reports]

repfiledelivery *n t rt username server-path port*

Deliver file based reports to an SSH server via SCP.

n = 1 to 999	report number
t = 1 to 65535	file upload time period (secs) (0=**disabled**)
rt = 1 to 65535	file upload retry period if uploads fail (secs) (0=**disabled**)
username	ssh username
server-path	ssh server host:path definition
port	ssh server TCP/IP port number, usually 22

Examples:

1. Set file delivery for report 1 :
   cmd repfiledelivery 1 60 10 report 199.199.199.99:~/reports 4222

See also: [File Based Reports]

repfiledir *local-path*

Sets the main folder for file-based reporting

local-path	folder for data files generated for file-based reporting (**default: /etc/reports**)

Examples:

1. Set main folder for file-based reports to /media. :
   cmd repfiledir /media/reports

See also: [File Based Reports]

repfilename *n name*

Sets the file prefix used for a file-based report.

n = 1 to 999	report number
name	file prefix to be used

Notes:

- File reports are named using a concatenation of this prefix, the report number, the modem mac address, and a timestamp (UNIX format).
  - eg. diginput-1-0010A1772797-1267216159

Examples:

1. Set file name for report 1 to diginput :
   cmd repfilename 1 diginput

See also: [File Based Reports]

repfileout *local-path*

Sets the outbox folder for file-based reporting

local-path	outbox folder for data files generated for file-based reporting (**default: /etc/reports**)

Examples:

1. Set outbox folder for file-based reports to /media :
   cmd repfileout /media/reports/outbox

See also: [File Based Reports]

repfilesize *kb*

Sets the maximum file size for file-based reporting

kb = 1-1024	maximum file size in KB (**Default 1024**)

Examples:

1. Set maximum file size for file-based reporting to 2 KB :
   cmd repfilesize 2048

See also: [File Based Reports]

repfiletimestamp *n*

Sets the timestamp added to data files for file-based reporting.

n = 0	No Timestamp added
n = 1	UTC timestamp added (e.g. "<1285133850><LF>") (**Default**)
n = 2	Formatted UTC timestamp added (e.g. "03/15/10 04:13:00<CR><LF>")
n = 3	Formatted UTC timestamp added (e.g. "03/15/10 04:13:00 ,")
n = 4	Formatted UTC timestamp added (e.g. "03/15/10 04:13:00 ")

Examples:

1. Set formatted UTC timestamp added to data file generated by file-based reporting :
   cmd repfiletimestamp 2

See also: [File Based Reports]

repfilezip *c*

Enables or disables the ability to compress data files generated by the file-based reporting system using different formats. Data files will be output in a required format with file names ending with the proper file extension.

c = 0	compression of data files = disabled (default)
c = 1	compression of data files = enabled GZIP format (.gz)
c = 2	compression of data files = enabled ZIP format (.zip)

Examples:

1. Enable compression of file-based reporting data files using GZIP format :
   cmd repfilezip 1

See also: [File Based Reports]

Firmware revision 1.3.0.1832

replocip *n iii.iii.iii.iii*

Sets the IP address of the local server connected to the modem?s LAN that the report will be sent to.

n = 1 to 999	report number
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	local IP address to receive local reports in decimal (**default 0.0.0.0**)

Notes:

- **firmware 3396** and later can broadcast local UDP messages.

Examples:

1. Report #1 will be sent to local IP address 192.168.1.21 :
   cmd replocip 1 192.168.1.21
2. Report #2 will be broadcasted on the local 192.168.1.0/24 subnet (**firmware 3396 and later**) :
   cmd replocip 2 192.168.1.255

See Also: [General Reports]

Firmware revision 1.3.0.1967

replocport *n xxxxx*

Sets the port number of the local server that the report will be sent to.

n = 1 to 999	report number
xxxxx = 0 to 65535	local port number in decimal

Examples:

1. Report #1 will be sent to local port 5005 :
   cmd replocport 1 5005

See Also: [General Reports]

reportscripts *n*

This command enables custom scripts to be triggered when reports are generated

n = 0	disable custom report triggered scripts (**default**)
n = 1	enable custom report triggered scripts

Notes:

- Custom scripts can be copied over to the modem via usb, scp, wget or ftp
- Custom scripts should be located in the directory /etc/reports/scripts, and must be named "reportN.sh" where N is

N = 1 to 999	for general reports 1 to 999
N = 1020 to 1027	GPS reports 1 to 8
N = 1040 to 1047	I/O reports 1 to 8

Examples:

1. Custom scripts located in */etc/reports/scripts* will be executed once the report number is triggered :
   cmd reportscripts 1

Firmware revision 1.3.0.1715

repremip *n iii.iii.iii.iii*

Sets the IP address of the remote server that the report will be sent to.

n = 1 to 999	report number
iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	remote IP address in decimal

Examples:

1. Report #1 will be sent to remote IP address 123.10.1.101 :
   cmd repremip 1 123.10.1.101

See Also: [General Reports]

repremport *n xxxxx*

Sets the IP port number of the remote server that the report will be sent to.

n = 1 to 999	report number
xxxxx = 0 to 65535	remote port number

Examples:

1. Report #1 will be sent to port 5005 on remote IP address set by [repremip] :
   cmd remport 1 5005

See Also: [General Reports]

repsms *n ppppppppppp|emailaddr*

Sets the destination of the report that is sent as an SMS message.

n = 1 to 999	report number
ppppppppppp	phone number which the SMS report will be sent to. For long distance calls, a ?1? needs to be added In front of the phone number.
emailaddr	email address which the SMS report will be sent to.

Notes:

- SMS features are only available for specific manufacturer, RF modules, cards or devices. Please contact Cypress Solutions for a complete list of products that support SMS functionality.

Examples:

1. Send report #1 as an SMS message to the specified phone number :
   cmd repsms 1 1234567890
2. Send report #2 as an SMS message to the specified email address :
   cmd repsms 2 me@?

See Also: [General Reports]

reptype *n l r s*

Sets the reporting type for local and remote servers.

n = 1 to 999	report number
l = 0	disables local report (default)
l = 1	asynchronous NMEA or ULCP messages over RS232
l = 2	asynchronous NMEA or ULCP messages with a ULCP header over RS232
l = 3	in-band NMEA or ULCP messages in a UDP Packet over Ethernet **Firmware 3211 and below**
l = 3	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets over Ethernet **Firmware 3232 and above**
l = 4	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets over Ethernet sent in binary format only
l = 5	in-band NMEA or ULCP messages in a TCP Packet over Ethernet **Firmware 3211 and below**
l = 5	in-band NMEA or ULCP messages with a ULCP header in individual TCP Packets over Ethernet **Firmware 3232 and above**
l = 6	file-based reports
r = 0	disables remote report (default)
r = 3	in-band NMEA or ULCP messages in a UDP Packet **Firmware 3211 and below**
r = 3	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets **Firmware 3232 and above**
r = 4	in-band NMEA or ULCP messages with a ULCP header and in individual UDP packets sent in binary format only
r = 5	in-band NMEA or ULCP messages in a TCP Packet **Firmware 3211 and below**
r = 5	in-band NMEA or ULCP messages with a ULCP header in individual TCP Packets **Firmware 3232 and above**
r = 6	email reports
r = 7	SMS reports
r = 8	in-band NMEA or ULCP messages requiring ACK messages from the remote WAN server in a TCP Packet
r = 9	in-band NMEA or ULCP messages requiring ACK messages from the remote WAN server in a UDP Packet
s = 0	disables the store and forward of report
s = 1	enables the store and forward of report

Notes:

- For **r = 7** (SMS reports), the total length of the report must not exceed 166 characters including <CR> and <LF>
- A remote report cannot be configured when using **l = 6** (File-based reporting).
- SMS features are only available for specific manufacturer, RF modules, cards or devices. Please contact Cypress Solutions for a complete list of products that support SMS functionality.
- For **r = 9** local reporting is disabled,ie reptype 1 1 9, the local report is disabled, if you need local reporting add another report with local reporting enabled, ie reptype 2 1 0

Examples:

1. Send report #4 as a UDP packet over Ethernet and over the wireless link, and will not store reports :
   cmd reptype 4 3 3
2. Send report #2 as a UDP packet over Ethernet and as an SMS message to the SMS destination set using the repsms command, and will enable the store and forward of reports :
   cmd reptype 2 3 7 1

See Also: [General Reports]

rfon

This command is used to reset the RF switch status to its default state with the RF cell device enabled.
The RF cell device is enabled by default whenever a [cmd factory full] is issued.

This command does not require any arguments.

A [cmd save] and a power cycle are required for this command to take effect.

---

see also: [rfswitch]

rfstats

Query various RF statistics

Notes:

- This is a read-only command

Examples:

1. Query RF statistics :
   cmd rfstats

See also: [Cellular]

rfswitch x

This command is used to enable or disable the RF switch feature on the CTM-200.
The RF switch feature is disabled by default whenever a [cmd factory] is issued.

x = 0 disable RF switch feature (default)
x = 1 enable RF switch feature

Examples:

1. Enable RF switch feature

```
cmd ctm15x
OK
cmd rfswitch 1
OK
```

A [cmd save] and a power cycle are required for this command to take effect.

---

see also: [ctm15x]

rmtssh *n*

Enables or disables remote SSH access to the modem.
If enabled, it will be possible to access the modem with a SSH client, using the current IP address allocated to the modem by the network.

n = 0	remote access = disabled (default)
n = 1	remote access = enabled

Examples:

1. enable remote access to the modem using SSH :
   cmd rmtssh 1

See also: [Local Remote Access]

rmttelnet

This command configures the modem to respond to incoming telnet commands over the wireless network.
The modem must be connected to a wireless network.

n=0 remote telnet = disabled (default)

n=1 remote telnet = enabled

The current state of remote telnet setting can be queried by using the **rmttelnet** command without pararmeters.

Examples:

cmd rmttelnet 1 sets the modem to respond to incoming telnet commands

cmd rmttelnet queries the modem?s setting for remote telnet access

A [cmd apply] followed by a [cmd save] are required for this command to take effect.

rmtweb *n*

Enables or disables remote access to the embedded web server feature of the modem.
If enabled, it will be possible to access the modem's embedded web pages by using the current IP address allocated to the modem by the network.

n = 0	remote access = disabled (default)
n = 1	remote access = enabled

Examples:

1. enable remote access to the modem?s web pages :
   cmd rmtweb 1

See also: [Local Remote Access]

rssi

This command queries to the current wireless network signal strength seen by the modem for both its Primary and Secondary networks.
The values are given in dBm in the range, for example: -105dBm (poor), to -60dBm (excellent).

Notes:

- This command is not supported by all wireless network cards and modules.
- This is a read only command.
- When **cmd universal 1** is configured then **cmd rssi** returns **0 dBm** for both Primary RSSI and Secondary RSSI.

Examples:

1. Query the current network signal strengths seen by the modem :
   cmd rssi

See also: [Cellular]

saltreport *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for the chlorobyte salt-spreader interface triggered reports.

r = 0	disables the report
r1 to r8 = 1 to 999	report number

Notes:

- When saltreport is configured to use a report, it appends to the already existing messages configured in the report a modified [114] message.

Examples:

1. use report 2 for salt-spreader interface triggered reports, adds a standard message 114 as a message :
   cmd saltreport 2
   cmd repaddmes 2 114

report output:

```
$PGPS,000000.00,V,0000.0000,N,00000.0000,E,000.0,000.0,000000,+00000,0,09604890958*42
$PGPS,000000.00,V,0000.0000,N,00000.0000,E,000.0,000.0,000000,+00000,0,131213141516171819202122232425262728293031*7E
```

In the above example the first line is the default [114] message, the second line shows the [114] message but with the salt spreader information instead of the modem ID. Note, the message type [114] does not have to be explicitly added as a message, this is handled automatically by the **saltreport** command.

See Also: [Salt Reports], [General Reports]

sat enable *n*

Control satellite availability.

n = 0	Disable and power off satellite (**Default**)
n = 1	Enable and power on satellite
n = 2	Dynamic mode (controlled by cmd sat pwr and firmware, **default off/disabled**)

Examples:

1. Enable and power on satellite :
   cmd sat enable 1

See also: [Satellite]

Firmware revision 2.0.5.3256

sat flush

Clears outbound satellite messages.

Examples:

1. Clear outbound satellite messages.
   cmd ctm15x
   cmd sat flush

See also: [Satellite]

Firmware revision 2.0.5.3256

sat force *n*

Bitmapped value selecting what type of message will force satellite ISU to power ON. Used with **cmd sat enable 2**. Pendant PANIC message is **ON by default** to ensure Pendant PANIC messages are sent out.

n = 0	No message type will force satellite ISU to power ON
n = 1	Pendant?s PANIC message will force ISU to power ON (**Default**)

Examples:

1. Force satellite to be enabled in dynamic mode when Pendant PANIC messages are being sent :
   cmd sat force 1

See also: [Satellite]

Firmware revision 2.0.5.3361

sat ip *iii.iii.iii.iii*

Configure remote server's IP to send messages received over satellite to, as well as to receive messages from to pass on via satellite. Uses TCP. Note that user must configure CTM's PAD server as TCP PAD server if used for PAD mode.

iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	Remote IP address in decimal (**Default 192.168.1.1**)

Examples:

1. For use with PAD mode (must use a local ethernet IP and not 127.0.0.1) :
   cmd sat ip 192.168.1.1

See also: [Satellite]

Firmware revision 2.0.5.3256

sat mt *n*

Set minimum time between identical report numbers.

n = 0 to 65535	Minimum time in minutes (**Default 10**)

Examples:

1. Allow reports of the same number to be sent over satellite within 20 minutes of each other :
   cmd sat mt 20

See also: [Satellite]

Firmware revision 2.0.5.3256

sat port *xxxxx*

Configure remote server's port to send messages received over satellite to, as well as to receive messages from to pass on via satellite. Uses TCP. Note that user must configure CTM's PAD server as TCP PAD server if used for PAD mode and to set **sat port** equal to **pad port**.

xxxxx = 0 to 65535	Remote port in decimal (**Default 23002**)

Examples:

1. For use with PAD mode (CTM using cmd pad port 5005) :
   cmd sat port 5005

See also: [Satellite]

Firmware revision 2.0.5.3256

sat pwr *n*

Control satellite availability when using **cmd sat enable 2**.

n = 0	Disable satellite (**Default**)
n = 1	Enable satellite

Examples:

1. Enable satellite reports (e.g. for failover mode) :
   cmd sat pwr 1

See also: [Satellite]

Firmware revision 2.0.5.3256

sat reset

Resets satellite tx/rx counter to 0.

Examples:

1. Reset transmission counter.
   cmd ctm15x
   cmd sat reset

See also: [Satellite]

Firmware revision 2.0.5.3256

sat stats

Query various satellite statistics

Notes:

- This is a read-only command

Examples:

1. Query satellite statistics :
   cmd sat stats

See also: [Satellite]

Firmware revision 2.0.5.3256

satbackup *b bt g gt o*

Sets the option to switch to a backup satellite modem if the cellular network?s coverage is poor.
The satellite modem power must be driven by a modem output for this feature to work.
The user defines the RSSI(receive signal strength) threshold to initiate the switchover, the timeouts and the output number to use.
When the RSSI value falls below the bad RSSI threshold for a certain timeout period, an output will be set.
When the RSSI value rises above or equal to the good RSSI threshold for a certain timeout period, an output will be cleared.

Notes:

- This command is only available on data cards/modules that provide RSSI information to the modem. Contact Cypress Solutions for a complete line of supported data devices

b = -1 to -125	Bad RSSI threshold in dBm; requires the negative sign (**0 disable**)
bt = 0 to 65535	Bad RSSI timeout in seconds; if the RSSI is less than the bad threshold for the timeout period, than set the output.
g = -1 to -125	Good RSSI threshold in dBm; requires the negative sign (**0 disable**)
gt = 0 to 65535	Good RSSI timeout in seconds; if the RSSI is greater than or equal to the good threshold for the timeout period than clear the output.
o = 1 to 4	Output number. (**Default 1**)
o = 5	Output on DSR on port 1

Examples:

1. Set the bad RSSI threshold to -100dBm with a timeout of 30 seconds; set the good RSSI threshold to -95dBm with a timeout of 30 second; trigger output 2 :
   cmd satbackup -100 30 -95 30 2

See also: [General Purpose IO]

cmd save

Save modem configuration to non-volatile memory.

Notes:

- A single **cmd save** should be entered after a series of commands are configured, the entire session will be saved.

Examples:

1. Save current configuration:
   cmd save

See also: [General]

sendreport *n x [x2][x3][x4]*

Sends a "One-Shot" report instantly. If a report already exists, the contents of sendreport are appended to the pre-existing report.

Notes:

- Messages will be sent in a report in the same order that they are added.
- ULCP header messages will be sent as individual UDP packets ? NMEA format messages will be combined into a single UDP packet.

n = 1 to 999	general report number
n = 1020 to 1027	GPS reports 1 to 8
n = 1040 to 1047	I/O reports 1 to 8
x	message type to be added, valid message types must be used - see [Report Messages]

Examples:

1. Send message type #3 #16 with general report #4 instantly :
   cmd sendreport 4 3 16
2. Send message type #3 with gps report #2 instantly (*1021*) :
   cmd sendreport 1021 3'

See Also: [General Reports]

Firmware revision 2.0.3.2256

showconfig [-quiet *emailaddr*]

Returns the current configurations of the CTM-200 gateway.

Notes:

- **cmd showconfig** without parameters returns the configuration of the commands as they were entered.
- Using **cmd showconfig -quiet *emailaddr*** will deliver the gateway's configuration settings to a specified email address. Note that an email server is required ? see [emailsrv].
- The output of **showconfig** is written to a script file **/tmp/config.sh** and to the console, both of which can be used to configure the gateway.
  The below commands are not supported using **showconfig**:
  - cmd odometer
  - cmd smstext
  - cmd enghours
  - cmd data
  - cmd event add
  - cmd ratesel
  - cmd telnetpswd

Examples:

1. Return the current gateway configuration settings :
   cmd showconfig
1. Email the current gateway configuration settings to the specified address :
   cmd showconfig -quiet me@?

See also: [Diagnostics and Logging]

---

cmd showconfig -quiet *emailaddr*- Firmware revision 2261

showstate

Returns the current state of the modem.

Notes:

- This is a read only command.
  showstate returns the modem state:
  - firmware revision
  - modem ESN
  - modem ID
  - modem IP address
  - odometer
  - engine hours
  - RF Switch output mode, 0 = RF device connected or connecting, 1 = RF device off, awaiting switch input.
  - SMS destination number
  - SMS text
  - amount of data transmitted and received over the wireless data link

Examples:

1. Query showstate :
   cmd showstate

Firmware Revision 1.2.2 (rev. 1480)

sms enable *n*

This command configures the CTM-200 to accept SMS commands.

n = 0	Disable SMS configuration access
n = 1	Enable SMS configuration access (**default**)

Notes:

- This command only applies to devices that support SMS. Please contact Cypress Solutions for more details.

Examples:

1. Disable SMS configuration support on the CTM-200 :
   cmd sms enable 0

See also: [SMS]

Firmware revision 2.0.5.3153

sms friends *n ppppppppppp*

This command is used to allow SMS messages only from phone numbers manually specified. All other phone numbers will be blocked from communicating to the modem via SMS.

n = 1 to 8	up to 8 phone numbers can be allowed
ppppppppppp	phone number

Notes:

- by default, all phone numbers are allowed access to the modem via SMS.

Examples:

1. SMS messages from phone number 16041234567 will be allowed, any messages from other phone numbers will be blocked :
   cmd sms friends 1 16041234567
2. SMS messages from phone number 16041112223 and 16044445556 will be allowed, any messages from other phone numbers will be blocked :
   cmd sms friends 1 16041112223
   cmd sms friends 2 16044445556

See also: [SMS]

sms fwdreport *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for forwarding incoming SMS messages received by the CTM-200 gateway.

This feature can be used to configure the CTM-200 as an SMS gateway that forwards messages from SMS-enabled devices to the CTM-200's reporting types (e.g. local serial port, local/remote TCP or UDP servers, or email/SMS destinations).

r1 to r8 = 1 to 999	report number
r1 to r8 = 1020 to 1027	**(Firmware 3034 and above)** GPS reports 1 to 8
r1 to r8 = 1040 to 1047	**(Firmware 3034 and above**) I/O reports 1 to 8

Notes:

- The SMS sender's phone number is included in the forwarded SMS messages.
- SMS configuration commands ($0<ctm command> or $1<ctm command>) are not forwarded by this feature.
- SMS features are only available for specific manufacturer, RF modules, cards or devices. Please contact Cypress Solutions for a complete list of products that support SMS functionality.

Examples:

Forward incoming SMS messages to a UDP server

```
cmd repremip 1 1.2.3.4
cmd repremport 1 8888
cmd reptype 1 0 3
cmd sms fwdreport 1
```

Forward incoming SMS messages to a TCP server

```
cmd repremip 1 1.2.3.4
cmd repremport 1 8888
cmd reptype 1 0 5
cmd sms fwdreport 1
cmd tcppersist 1
```

Forward incoming SMS messages to an email address ([emailsrv] provided by carrier is required)

```
cmd emailsrv 1.2.3.4
cmd repemail 1 me@home.com
cmd reptype 1 0 6
cmd sms fwdreport 1
```

See also: [SMS], [General Reports]

Firmware version 2.0.5.2916

smssend

Used to send the previously setup SMS message

Note:

- SMS features are only available for specific manufacturer, RF modules, cards or devices. Please contact Cypress Solutions for a complete list of products that support SMS functionality.

Examples:

1. send the SMS message :
   cmd smssend

See also: [SMS]

smstext *string delimiter*

Used to enter the text message of the SMS.

string	text message(max 166 chars)
delimiter	sequence of a blank line followed by a carriage return and then the sequence ?.?

Notes:

- SMS features are only available for specific manufacturer, RF modules, cards or devices. Please contact Cypress Solutions for a complete list of products that support SMS functionality.
- **cmd smstext** cannot be used from a serial console.
- The delimiter is used to indicate an end of text message.
- Text message is saved in volatile memory (ie. Message will be removed when power cycled).

Examples:

1. create a volatile SMS message, the last line indicates the delimiter :
   cmd smstext <CR>
   Hi <CR>
   This is test <CR>
   message<CR>
   from Bob<CR>

   .<CR>

See also: [SMS]

smsto *ppppppppppp*

This command is used to set the phone number of the SMS text message to be sent.

ppppppppppp	phone number which the text message will be sent to. For long distance calls, a ?1? needs to be added in front of the phone number.

Notes:

- SMS features are only available for specific manufacturer, RF modules, cards or devices. Please contact Cypress Solutions for a complete list of products that support SMS functionality.
- The phone number is saved in volatile memory (ie. changes will not be saved when power cycled)

Examples:

1. sets the phone number to send the SMS :
   cmd smsto 1235551212
2. returns the phone number this command is set to :
   cmd smsto

See also: [SMS]

smsview

Query the message entered via [smstext] command.

Note:

- SMS features are only available for specific manufacturer, RF modules, cards or devices. Please contact Cypress Solutions for a complete list of products that support SMS functionality.
- This is a read only command.

Examples:

1. returns the text message to be sent :
   cmd smsview

See also: [SMS]

snfdelay *t rssi*

This command sets the store-and-forward delay time and minimum signal strength (RSSI) required before stored messages are forwarded.

t = 1 to 65535	Delay time in seconds (**default 20**)
rssi	rssi threshold (**default -95**)

Notes:

- Valid RSSI threshold should be a value between -95 and 0
- message forwarding may not occur exactly at the snfdelay interval specified, and stored messages will only start forwarding when network conditions are deemed acceptable.

Examples:

1. Set the delay time before forwarding SNF data to 60 seconds with signal strength >= -80 dBm :
   cmd snfdelay 60 -80

See also: [Store and Forward]

snfflush

Flushes and resets store and forward NVRAM.

Notes:

- This command may have to be entered multiple times before the SNFlog is flushed.

Examples:

1. reset store and forward values :
   cmd snfflush'

See also: [Store and Forward]

snflog *n* | *all*

Used to display the contents of the store and forward (SNF) database locally thru a serial console/terminal, and the status of the log entries.

This is a read only command.

n = 1 to N	dumps the first **n** reports from the SNF database
n = -1 to -N	dumps the last **n** reports from the SNF database
all	dumps all reports from the SNF database

Examples:

1. display the first 10 SNF database reports :
   cmd snflog 10
2. display the last 10 SNF database reports :
   cmd snflog -10
3. display the SNF database status :
   cmd snflog

See also: [Store and Forward]

Firmware revision 2.0.5

snfonsd *n*

This command configures the CTM-200 to use internal or external storage (microSD) for TCP store and forward (TCPSNF) system.

n = 0	Internal (default)
n = 1	External on microSD

Notes:

- If external storage on microSD is selected, reports will no longer be saved locally on CTM200 itself and previous reports saved locally won?t be resent until internal storage option is reselected. Similarly, if internal storage is selected, reports saved on the microSD card won?t be resent until external storage option is reselected.
- Upgrading CTM200?s firmware will remove all TCPSNF reports saved locally on the CTM200. Use external storage on microSD if this is a critical issue.

Examples:

1. To use external storage (microSD) :
   cmd snfonsd 1

See also: [Store and Forward]

Firmware revision 2.0.5.3105

snmp *n*

This command configures the CTM-200 to respond to incoming simple network management protocol (SNMP) requests over the local or wireless network.

n = 0	Disable SNMP server (**default**)
n = 1	Enable SNMP server

Notes:

- The CTM-200's SNMP server supports SNMP versions 1 and 2c.
- The CTM-200's SNMP server listens on UDP port 161 for SNMP requests.
- Please contact Cypress Solutions for the CTM-200 SNMP management information base (MIB) file required by SNMP clients and for the list of supported SNMP parameters.

Examples:

1. Enable SNMP support on the CTM-200 :
   cmd snmp 1

See also: [SNMP]

Firmware revision 2.0.4.2494

spc *nnnnnn*

This command is used to enter the modem?s CSL (Client Subsidy Lock) as part of the network activation commands prior to loading the modem?s 10-digit phone number using the [dir] command.
The 6-digit lock code is used by the modem?s embedded module to compare against the pre-loaded 6-digit CSL. This number will be provided by the service provider at the time of service activation.

nnnnnn	6-digit lock code

Examples:

1. set the modem?s SPC to 123456 :
   cmd spc 123456

[Cellular]

speedth *s t*

Sets the speed threshold for automatically enabling the RF module of the modem when it has been previously disabled.
Turns off output **#4** when it has been previously turned on.

Notes:

- The RF module of the modem is disabled by using an external switch box(supplied by Cypress Solutions) connected to the modem when the modem is used in areas sensitive to RF interference.

s	speed threshold (kph). (**Default 30**)
t	time in seconds (**Default 3**)

Examples:

1. set the RF module of the modem to automatically turn on when the speed reaches 50 km/h for at least 5 seconds :
   cmd speedth 50 5

See also: [Power Management]

sshkey *dss* | *rsa*

Generate a SSH public/private key pair.

dss	Generate a 1024 bit DSS key pair
rsa	Generate a 1024 bit RSA key pair

Examples:

1. Generate DSS public/private key pair :
   cmd sshkey dss

root@OpenWrt:~# cmd sshkey dss
Will output 1024 bit dss secret key to '/etc/dropbear/id_dss'
Generating key, this may take a while...
Public key portion is:
ssh-dss
AAAAB3NzaC1kc3MAAACBAKV8x80K0wnyc4Ia/NiD0BTZLhPYVPO8FhB3kWzLOdB99SyQBgl6tXaYvPXT+rV24qzmJaNIDlwMAsJRxp86Jki/WogktrN1jjjl8bnwrvjvM1
root@OpenWrt
Fingerprint: md5 6b:06:6e:f4:2e:0e:58:21:12:1d:f8:51:25:2a:a5:6d
OK

See also: [File Based Reports]

sshport *port*

Sets the port for ssh access (both local and remote).

port = 1 to 65535	port to be used for ssh (**default 22**)

Examples:

1. Set ssh port to 3322 :
   cmd ssh 3322

See also: [Local Remote Access]

sshtimeout *n*

Sets the timeout period for a ssh session with no activity.

n = 0 to 65535	timeout time, in seconds (**default 60**)

Examples:

1. Disable ssh timeout :
   cmd sshtimeout 0

See also: [Local Remote Access]

stm upgrade *f [u] [n] [p]*

Updates the CTM200's Mini Micro FW. The **"cmd stm upgrade"** command requires 4 parameters when accessing an FTP server, 2 parameters when accessing an HTTP server or scripts locally.

f = imagefile.tar	Name of the file containing the firmware image
u = <blank>	Same as localhost
u = localhost	Localhost, image must be in /tmp
u = url	URL, can be IP address. Prefixed by ftp:// or http://, if no prefix is specified (eg. cypress.bc.ca) then ftp:// is used.
n = username	Username for FTP server (Optional)
p = password	Password for FTP server (Optional)

Notes:

- Username and password can only contain alphanumeric characters.

Examples:

1. From Cypress FTP server:

```
cmd stm upgrade CTM2xxMiniMicro-CRC-R99.bin.tar cypress.bc.ca cypress PASSWORD
cmd stm upgrade CTM2xxMiniMicro-CRC-R99.bin.tar ftp://cypress.bc.ca cypress PASSWORD
```

1. From Cypress URL site.:

```
cmd stm upgrade CTM2xxMiniMicro-CRC-R158.bin.tar http://www.cypress.bc.ca/repository/openctm/eng13
cmd stm upgrade http://www.cypress.bc.ca/repository/openctm/eng13/CTM2xxMiniMicro-CRC-R158.bin.tar      <---must be on t
```

1. From the local folder, /tmp:

```
cmd stm upgrade CTM2xxMiniMicro-CRC-R158.bin.tar localhost
```

See also: [Diagnostics and Logging], [Firmware Upgrade and Configuration]

Firmware revision 2.0.1.2221

swipegpio *n*

Sets the GPIO row to be used.

n = 0	Use GPIO's top row (inputs 3/5 and outputs 1/3)(default)
n = 1	Use GPIO's bottom row (inputs 4/6 and outputs 2/4)

Examples:

1. Set CTM-200 to use GPIO's top row for iButton interface :
   cmd swipemode 11
   cmd swipegpio 0
1. Set CTM-200 to use GPIO's bottom row :
   cmd swipegpio 1

See also: [RFID Card Reader Support]

swipeid

This command queries query the ID of the last swiped card.
The swipe ID is read only and cannot be altered.

Examples:

1. Query the last card swiped when using the serial HID or GPIO swipe card interface

```
cmd swipeid
001F084EED1E80
OK
```

1. Query the last card swiped when using the serial iButton swipe card interface

```
cmd swipeid
iD1000012E33E7901
OK
```

See Also: [[swipemode]

This command was added to the firmware in revision R1.2.2 (rev. 1547)/R1.3.0 (rev. 1547)

swipemode *n*

Sets the swipe card interface to be used with the modem.

n = 0	Serial HID swipe card interface (default), requires **cmd mode 9**
n = 1	Serial iButton swipe card interface, requires **cmd mode 9**
n = 10	GPIO HID swipe card interface, works in any [mode] and takes priority in **cmd mode 9**
n = 11	GPIO iButton interface

Examples:

1. Set modem to use the GPIO HID swipe card interface :
   cmd swipemode 10
2. Set CTM200 to use iButton interface connected to GPIO port :
   cmd swipemode 11

See Also: [RFID Card Reader Support]

swipereport *r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for swipe card reader triggered reports.

r = 1 to 999	report number

Note:

- When **swipereport** is configured to use a report, it appends to the already existing messages configured in the report a modified 114 message. The appended message contains the ID of the swipe card detected by the swipe card reader. [mode] must be configured correctly to allow the swipe card reader to communicate with the modem.

Examples:

1. uses report 2 with store and forward enabled for swipe card reader triggered reports, adds a standard message 114 as a message :
   cmd repaddmes 2 114
   cmd swipereport 2

report output:

```
$PGPS,171134.00,A,4915.3868,N,12259.8049,W,000.0,000.0,170609,+00004,5,09604890958*4A
$PGPS,171134.00,A,4915.3868,N,12259.8049,W,000.0,000.0,170609,+00004,5,09604890958,039-30391,V*33
```

In the above example the first line is the default [114] message, the second line shows the appended swipe card ID information added to the message. Note, the message type [114] does not have to be explicitly added as a message, this is handled automatically by the **swipereport** command.

See Also: [RFID Card Reader Support]

syslog *n*

Provides a mechanism to retrieve the log of system events recorded by the modem.

n = 0 to 65535	number of system log records to return. Leaving **n** blank will return the entire contents of the system log.

Notes:

- The system log is stored in volatile memory so it will be lost when power is cycled on the modem.

Examples:

1. return the last 10 events stored in the system log :
   cmd syslog 10
2. return all events stored in the system log :
   cmd syslog

See also: [Diagnostics and Logging]

taipchecksum *n*

Enables/disables checksum in Trimble ASCII Interface Protocol messages. Checksum field will be used in GPS TAIP [PV]/[LN] message.

n = 0	disable checksum in TAIP messages (default)
n = 1	enable checksum in TAIP messages

Examples:

1. Enable checksum in TAIP messages :
   cmd taipchecksum 1

See also: [TAIP Reports]

Firmware revision 2.0.5-2954

taipid *DDDD*

Sets Trimble ASCII Interface Protocol ID. TAIP ID will be used in GPS TAIP [PV]/[LN] message.

DDDD	a four-character alphanumeric code (**default 0000**)

Examples:

1. Set TAIP ID as 'Abc1' :
   cmd taipid Abc1

See also: [TAIP Reports]

Firmware revision 2.0.5-2954

taipuseid *n*

Enables/disables reporting of ID in Trimble ASCII Interface Protocol messages. TAIP ID will be used in GPS TAIP [PV]/[LN] message.

n = 0	disable reporting of ID in TAIP messages (**default**)
n = 1	enable reporting of ID in TAIP messages

Examples:

1. Enable reporting of ID 'Abc1' in TAIP messages :
   cmd taipid Abc1
   cmd taipuseid 1

See also: [TAIP Reports]

Firmware revision 2.0.5-2954

tcppersist *n*

This command configures the CTM-200 to maintain persistent TCP connections for configured TCP reports.

n = 0	disabled (**default**)
n = 1	enabled

Examples:

1. Enable persistent connections for TCP reports
   cmd tcppersist 1

Firmware revision 1.3.0.2251 and 2.0.3.2322.

telnetport *n*

Sets the port for telnet access (both local and remote).

n = 1 to 65535	port to be used for telnet (**default 23**)

Examples:

1. Set telnet port to 33 :
   cmd telnetport 33

See also: [Local Remote Access]

telnetpswd *n*

Sets password for telnet access (both local and remote) and ssh access (both local and remote).

n	maximum 40-character alpha-numeric password

Notes:

- This command is not visible in a [showconfig] ouput

Examples:

1. Set telnet/SSH password to 'cypress' :
   cmd telnetpswd cypress

See also: [Local Remote Access]

telnettimeout *n*

Sets the timeout period for a telnet session with no activity.

n = 0 to 65535	timeout time in seconds (**default 60**)

Examples:

1. Set telnet timeout to 120 seconds :
   cmd telnettimeout 120
2. Disable telnet timeout :
   cmd telnettimeout 0

See also: [Local Remote Access]

timesync *t*

Set the period in seconds when the modem's system time and the power management controller's time are synchronized with one or more external sources:

- Valid GPS ([gpstime])
- Network time protocol (NTP) built-in client ([ntptime])
- Cellular network time ([networktime])

|t = 0 to 65535	synchronization period in seconds (**default 3600**)

Examples:

1. Update system time and power management controller time as fast as possible :
   cmd timesync 0
2. Update system time and power management controller time every 2000 seconds :
   cmd timesync 2000

See also: [Time Synchronization]

Firmware revision 1.3.0.1729

timezone *tz*

Set the system timezone.

tz	a valid timezone from this list [timezones].

Examples:

1. Set timezone to PST :
   cmd timezone PST8PDT

See also: [Time Synchronization]

Firmware revision 2.0.4.2595

universal *n*

Enable/disable universal card mode override.

n = 0	Disable universal card mode
n = 1	Enable universal card mode

Notes:

- **All cards will be treated as "universal" by default if not detected as Sierra Wireless or Kyocera.**
  With **cmd universal 1**:
  - phone card/module specific diagnostics for Sierra Wireless or Kyocera are bypassed:
    - **cmd rssi** returns **0 dBm** for both primary RSSI and secondary RSSI
    - **cmd esn** returns **00000000000**
  - network registration detection is not required to initiate pppd dialout
  - the ESN field of [NMEA Message Type 03, PMID] is set to the modem ID configured in **cmd modemid**

Examples:

1. To enable universal card mode :
   cmd universal 1

See also: [univwd]

univwd *m url/report*

Configure the Universal Watchdog.

m = 0	disabled
m = 1	detect increase in received packets.
m = 2	ping specified url
m = 3	send specified report

Examples:

1. Set universal watchdog into mode 3, which will use general report 1 to generate ping activity:
   cmd univwd 3 1

See Also: [Watchdog Timers]

univwdtimer *n p*

Sets the timer value for the universal watchdog timer.

n = 1 to 65535	watchdog timer interval in seconds
p = 1 to 60	watchdog ping interval in seconds, valid for [univwd] modes = 2 and 3

Examples:

1. Set universal watchdog timer interval to 300 seconds and watchdog ping interval to 30 seconds :
   cmd univwdtimer 300 30

See also: [Watchdog Timers]

upgradefw *imagefile.tar url username passwd*

Remote upgrade of the firmware (kernel and root filesystem images).

imagefile.tar	the name of the file containing the firmware image
url	can be **localhost**, or the address of the FTP or HTTP server, can also be an IP address, prefixed by ftp:// or http:// respectively; if no prefix is specified (eg. cypress.bc.ca) then ftp:// is used.
username	username to access FTP server (ignored when **url** is prefixed by http:// or **url** is **localhost**)
passwd	password to access FTP server (ignored when **url** is prefixed by http:// or **url** is **localhost**)

Notes:

- When **localhost** is specified as the **url**, the image file must be located in **/tmp** on the modem.

Examples:

where *openctm-1.3.0-r1590.tar* is the image file, *cypress.bc.ca* is the FTP server, *guest* is the username of the FTP server, and *guestpw* is the password of the FTP server :

```
cmd upgradefw openctm-1.3.0-r1590.tar cypress.bc.ca guest guestpw
```

where *openctm-1.3.0-r1590.tar* is the image file, and */tmp* is the location of the image file :

```
cmd upgradefw openctm-1.3.0-r1590.tar localhost
```

where *openctm_r2_0_1_2171.tar* is the image file and *http://www.cypress.bc.ca/repository/openctm/ctm200/bin/* is the HTTP path :

```
cmd upgradefw openctm_r2_0_1_2171.tar http://www.cypress.bc.ca/repository/openctm/ctm200/bin/
```

See also: [Device Management]

upgradesrv *a.a.a.a*

This command is used to set the IP address of a remote client that is authorized to run remote administration commands.

The RemoteAdminServer commands: [cmd showconfig], [cmd confupgrade] and [cmd pwr mode 2] are restricted to an authorized IP.

a.a.a.a = 0.0.0.0 to 255.255.255.255	IP address of the authorized IP client
a.a.a.a = 0.0.0.0	disables all remote clients
a.a.a.a = 255.255.255.255	enables all remote clients

Examples:

1. Set the upgrade server IP address to 209.121.68.211 :
   cmd upgradesrv 209.121.68.211

See also: [Device Management]

usepeerdns *n*

This command is used to enable or disable the CTM-200 gateway from obtaining its DNS nameserver IP addresses from the carrier when it connects to the network.

n = 0	disable obtaining DNS nameserver IP addresses from the carrier
n = 1	enable obtaining DNS nameserver IP addresses from the carrier (**default**)

Examples:

1. Enable obtaining DNS nameserver IP addresses from the carrier :
   cmd usepeerdns 1
2. Disable obtaining DNS nameserver IP addresses from the carrier :
   cmd usepeerdns 0

See also: [Cellular]

Firmware revision R1.3.x.1894

user *name*

Sets the username used for wireless network access via simple IP. This is often in the format of **[phone number]@[carrier].com**.

name	a maximum of 40-character alpha-numeric username

Examples:

1. sets the username to 6045551234@? :
   cmd user 6045551234@?

See Also: [Cellular]

vcc

Returns the current value of the modem?s supply voltage.

Notes:

- This is a read only command.

Examples:

1. Query the supply voltage :
   cmd vcc

See also: [VCC Reports]

vcccond *n o [a.a] [mt]*

This command is used to set the condition(s) that would trigger a supply voltage level report. The conditional parameter is used to indicate how all following parameters will be used to determine if a report is triggered. Use the Off setting to disable the report.

n = 1 to 8	supply voltage level condition trigger
o=0	trigger disabled (**default**)
o=1	trigger while supply voltage is below threshold
o=2	trigger while supply voltage is above threshold
o=3	trigger on transition (whenever supply voltage threshold is passed) Above threshold->below threshold or below threshold->above threshold.
a.a = 6.0 to 36.0	threshold voltage, in volts (**default 9.0**) (**CTM-200**)
a.a = 9.0 to 36.0	threshold voltage, in volts (**default 9.0**) (**CTM-15X**)
mt = 0 to 65535	maximum reporting rate in seconds (minimum time between reports). (**Default 60**)

Examples:

1. Trigger vcccond 1 every 60 seconds while supply voltage is below the threshold voltage of 9.0 volts :
   cmd vcccond 1 1
2. Triggers vcccond 2 every 60 seconds while supply voltage is below the threshold voltage of 7.0 volts :
   cmd vcccond 2 1 7.0

See Also: [VCC Reports]

vccreport *n r1 [r2] [r3] [r4] [r5] [r6] [r7] [r8]*

This command sets the report(s) to be used for supply voltage level triggered reports.

n = 1 to 8	supply voltage level trigger condition
r1 to r8 = 1 to 999	report number
r1 to r8 = 0	disables the report

Examples:

1. Configure VCC threshold trigger to use reports #2 and #33 for supply voltage level trigger condition 1 :
   cmd vccreport 1 2 33

See Also: [VCC Reports]

ver

Queries the currently installed firmware version of the modem.

Examples:

1. Query the current firmware version :
   cmd ver

See also: [Diagnostics and Logging]

Firmware revision 1.2.0 (rev. 1140)

vpnc *n*

Enable the VPNC vpn client application

n = 0	Disabled (Default)
n = 1	Enable

Examples:

1. Enable VPNC vpn client :
   cmd vpnc 1

vue ack *string*

Configure VUE service to send an acknowledgement string to the VUE device management server.

string	text string with no spaces

Note:

The payload of ***string*** is send as a variable to the "Text1" parameter part of the Generic GpsGate device mapper. Text1 can be mapped to Monitor Status where so reports can be generated that provide diagnostics for device management commands.

Examples:

1. Send *this_is_a_test* to the VUE device management server :
   cmd vue ack this_is_a_test

See also: [VUE]

Firmware revision 2.0.5.2897

vue period *n*

Configure the time period (in minutes) for the device to run VUE client, the CTM client management and configuration agent.

n = 0 to 65535	Time period, in minutes, between running VUE client. (**default 360 , or 6 hours**)

Notes:

- the periodic VUE client timer can be disabled by setting the value to 0, eg. **cmd vue period 0**
- this integrated command replaces the use of a system cron job for running VUE client, typically

Examples:

1. Set VUE client period to 15 minutes :
   cmd vue period 15

See also: [VUE]

Firmware revisions R2.0.5.3198

vue port *n*

Configure TCP server port for device used when VUE service is run in server mode.

n = 1 to 65535	TCP port number of listening port, (**default 30175**)

Examples:

1. Set VUE service in server mode to listen on TCP port :
   cmd vue port 12345

See also: [VUE]

Firmware revisions R1.3.0.2260 and R2.0.3.2260

vue pwrup *n*

Configure VUE client to run after device power up.

n = 0	disabled
n = 1	enabled (**default**)

Examples:

1. Set VUE client to run once on power-up :
   cmd vue pwrup 1

See also: [VUE]

Firmware revision 2.0.5.xxxx

vue remip *a.a.a.a*

Configure IP address of remote VUE server. When the VUE service is run in client mode, this command sets the IP address of the remote VUE server that is periodically checked for any pending commands. When the VUE service is run in server mode, this command sets the IP address of the remote VUE server that is authorized to run commands.

a.a.a.a = 0.0.0.0 to 255.255.255.255	IP address of the authorized server. (Default before firmware 3032 **64.46.40.148** after 3032 **vue.cypress.bc.ca**)
a.a.a.a = 0.0.0.0	disables all remote servers
a.a.a.a = 255.255.255.255	enables all remote servers

Examples:

1. Set remote VUE server IP address to 1.2.3.4 :
   cmd vue remip 1.2.3.4

See also: [VUE]

Firmware revision 1.3.0.2260 and 2.0.3.2260

vue remport *n*

Configure TCP port number of remote VUE server used when VUE service is run in client mode.

n = 1 to 65535	TCP port number of remote VUE server, in decimal (**default 11650**)

Examples:

1. Set VUE service in client mode to use TCP port 12345 :
   cmd vue remport 12345

See also: [VUE]

Firmware revision 1.3.0.2260 and 2.0.3.2260

vue service *n*

Configure VUE service to support remote device management from a VUE server. The CTM device communicates with the VUE server over a TCP connection.

n = 1	set VUE service to run in client mode (**default**)
n = 2	set VUE service to run in server mode

Notes:

- **n = 2** can only be used with CTM cellular devices that have non-routable IP addresses.

Examples:

1. Set CTM device to use VUE service in server mode :
   cmd vue service 2

See also: [VUE]

Firmware revision 1.3.0.2260 and 2.0.3.2260

wifi ap|client channel *n*

Set the wifi channel for client or access point (AP)

ap|client	configure **ap** or **client**
n = 1 to 11	Channel must be a channel number between 1 and 11
n = auto	Set wifi **client** channel to **auto**.

Notes:

- The maximum number clients that can connect to an AP at the same time is 7

Examples:

1. Set wifi AP channel to 11:
   cmd wifi ap channel 11

See also: [Wi-Fi Networks]

wifi ap|client country *country-code*

Set the regulatory domain for wifi radio communications.

ap|client	configure AP or client
country-code	Country code is a 2 character value chosen from the following list of [country codes]

Examples:

1. Set wifi AP country for Canada:
   cmd wifi ap country CA

See also: [Wi-Fi Networks]

wifi ap|client encryption *enctype*

Set wireless connection encryption type

ap|client	configure AP or client
enctype	one of **none**, **psk**, **psk2**, **tkip, wpa**

Note:

- The maximum number clients that can connect to an AP at the same time is 7

Examples:

1. Set wifi AP encryption to psk2 :
   cmd wifi ap encryption psk2

See also: [Wi-Fi Networks]

wifi ap|client hwmode *mode*

Set the hardware mode for the wifi radio.

ap|client	: configure AP or client
mode	: mode is one of the following: **11n**, **11ng**, **11bg**

Notes:

- The maximum number clients that can connect to an AP at the same time is 7

Examples:

1. Set wifi client hwmode for 11ng :
   cmd wifi client hwmode 11ng

See also: [Wi-Fi Networks]

wifi ap|client key *pre-shared-key*

Set the pre-shared-key for an encrypted wifi configuration.

ap|client	configure AP or client
pre-shared-key	a passphrase between 8 and 64 characters in length

Notes:

- The maximum number clients that can connect to an AP at the same time is 7

Examples:

1. Set wifi AP pre-shared key to 'CypressAccess' :
   cmd wifi ap key CypressAccess

See also: [Wi-Fi Networks]

wifi mac

This command can be used to query the MAC address of the CTM-200 wireless radio.

Examples:

1. Query MAC address of CTM-200 Wifi module :
   cmd wifi mac

See also: [Wi-Fi Networks]

wifi radiusport *n*

Set the port number for a wifi Radius authentication server

n = 0 to 65535	Radius server port number

Examples:

1. Set the Radius server port to 5678 :
   cmd wifi radiusport 5678

See also: [Wi-Fi Networks]

wifi radiusserver *iii.iii.iii.iii*

Set the IP address for a wifi Radius authentication server

iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	Radius server IP address in decimal

Examples:

1. Set the Radius server IP address to 199.99.22.21 :
   cmd wifi radiussrv 199.99.22.21

See also: [Wi-Fi Networks]

wifi ap|client ssid *SSID*

Set the SSID for the wifi connection.

ap|client	: configure AP or client
SSID	SSID of wireless access point

Notes:

- The maximum number clients that can connect to an AP at the same time is 7

Examples:

1. Set the wifi client SSID to CypressAP :
   cmd wifi client ssid CypressAP

See also: [Wi-Fi Networks]

wifi watchdog *n [t]*

Enable/disable wifi watchdog.

n=0	disable watchdog
n=1	enable watchdog
t=31 to 65535	Watchdog threshold time in seconds (**Default 120**)

Examples:

1. Enable wifi watchdog with a 5 minute threshold :
   cmd wifi watchdog 1 300

See also: [Wi-Fi Networks]

wlan dns *ipaddr*

Set a DNS namerserver IP address for the CTM-200 wifi client interface (WLAN).

ipaddr = 0.0.0.0 to 255.255.255.255	DNS IP address in decimal (default for **eth0** is **192.168.1.1**. Default for **eth1** is **192.168.2.1**)

Notes:

- This option is usually only required if the WLAN interface is configured to use a static IP address, see [wlan proto].

Examples:

1. Set the WLAN DNS namerserver IP address to **192.168.10.254**:
   cmd wlan dns 192.168.10.254

See also: [Wi-Fi Networks]

wlan enable *n*

Configure CTM cell/wi-fi operation mode

n = 0	Cell only
n = 1	Cell + Wifi Client
n = 2	Cell + Wifi Access Point
n = 3	Wifi Client only

Examples:

1. Enable wifi as Access Point (AP) on LAN :
   cmd wlan enable 2
2. Use wifi client only :
   cmd wlanenable 3

See also: [Wi-Fi Networks]

wlan gw *ipaddr*

Set a default gateway IP address for the CTM-200 wifi client interface (WLAN).

ipaddr = 0.0.0.0 to 255.255.255.255	gateway IP address in decimal (default: **eth0: 192.168.1.1** and **eth1: 192.168.2.1**)

Notes:

- **cmd wlan gw** should only be set if using **cmd wlan proto static**.

Examples:

1. Set the WLAN default gateway IP address to 192.168.10.254 :
   cmd wlan gw 192.168.10.254

See also: [Wi-Fi Networks]

wlan ip *ipaddr*

Set a static IP address for the CTM-200 gateway's wifi client interface (WLAN).

ipaddr = 0.0.0.0 to 255.255.255.255	WLAN IP address in decimal

Examples:

1. Set the WLAN IP address to 192.168.10.1 :
   cmd wlan ip 192.168.10.1

See also: [Wi-Fi Networks]

wlan netmask *iii.iii.iii.iii*

Sets the netmask of the CTM-200 gateway's wifi client interface (WLAN).

iii.iii.iii.iii = 0.0.0.0 to 255.255.255.255	WLAN netmask (**default: 255.255.255.0**)

Examples:

1. Set the WLAN netmask of the CTM-200 gateway's wifi client to 255.255.255.0 :
   cmd wlan netmask 255.255.255.0

See also: [Wi-Fi Networks]

wlan proto *type*

Define the network protocol for the CTM-200 wifi client interface (WLAN) to use DHCP or static IP address.

type = dhcp	DHCP client (**Default**)
type = static	static IP address

Notes:

- The current WLAN protocol can be queried by using **wlan proto**.
- if **static** protocol is used, the following WLAN options must also be configured: IP address [cmd wlan ip], netmask [cmd wlan netmask], gateway [cmd wlan gw]. And optionally: [cmd wlan dns].

Examples:

1. Set the WLAN protocol to static :
   cmd wlan proto static

See also: [Wi-Fi Networks]

wpan acktype *type*

Assigns an acknowledgment type for the Work Alone system.
There are two acknowledgment types:

type = m	CTM-200 type acknowledgment (**default**)
type = s	Server type acknowledgment

Notes:

- If a user initiates a ?Man Down Emergency? alert, the Pendant will provide the worker with either a **positive acknowledgment** or a **negative acknowledgment**.
- Entering **wpan acktype** with no arguments returns the current command configuration.
- CTM-200 type acknowledgment:
  A positive acknowledgment (ACK) means the CTM-200 has received the alert. If the Pendant has not received an acknowledgment from the CTM-200, the Pendant will continue to send PANIC/MPANIC messages until an acknowledgment(ACK) is received. (Pendant firmware V1.1 and later)
- Server type acknowledgment:
  A positive acknowledgment means that the server has received the alert from the CTM-200 and acknowledged back to the CTM-200 then to the Pendant. If the Pendant has not received an acknowledgment from the server, the Pendant will continue to send PANIC/MPANIC messages until it receives an acknowledgment(ACK). (Pendant firmware V1.1 and later)
- The remote server must also be configured to respond to messages from the CTM-200.

The message format sent from the CTM-200 is as follows:

```
$PPEN,0013A200402CB498,13,PANIC*03
```

- The acknowledgment that the CTM-200 expects from the server is as follows:

```
$PPQ,PAN,0013A200402CB498,13,ACK*36
```

The 16-digit hex number following the PPEN message is the Pendant ID and is unique to each Pendant.

Examples:

1. Configured as CTM-200 type acknowledgment :
   cmd wpan acktype m
1. Configured as server type acknowledgment :
   cmd wpan acktype s

See also: [Down Pendant]

Firmware revision 2.0.4.2560

wpan adddev *xx-xx-xx-xx-xx-xx-xx-xx*

Adds a WPAN device ID to the CTM-200?s registered WPAN devices list. Up to 16 WPAN IDs can be entered.

xx-xx-xx-xx-xx-xx-xx-xx	WPAN device ID (hex digits), hyphens are optional

Notes:

- Using **wpan adddev** without a device ID, queries all WPAN devices IDs currently registered in the CTM-200.
- The ID of FF-FF-FF-FF-FF-FF-FF-FF will allow any Pendant to talk through the CTM-200.

Examples:

1. Add WPAN device with this ID to the registered devices list :
   cmd wpan adddev 00-13-a2-00-40-08-58-5e
1. Above example with optional hyphens omitted :
   cmd wpan adddev 0013a2004008585e

See also: [Down Pendant]

Firmware revision 2.0.1.2221

wpan delall

Deletes all WPAN device IDs from the CTM-200?s registered WPAN devices list.

Examples:

1. Delete all WPAN devices from the registered devices list :
   cmd wpan delall

See also: [Down Pendant]

Firmware revision 2.0.1.2221

wpan deldev *xx-xx-xx-xx-xx-xx-xx-xx*

Deletes a WPAN device ID from the CTM-200?s registered WPAN devices list.

xx-xx-xx-xx-xx-xx-xx-xx	WPAN device ID (hex digits), hyphens are optional

Examples:

1. Delete WPAN device with this ID from the registered devices list :
   cmd wpan deldev 00-13-a2-00-40-08-58-5e
1. Above example with optional hyphens omitted :
   cmd wpan deldev 0013a2004008585e

See also: [Down Pendant]

Firmware revision 2.0.1.2221

wpan dist *n*

n = 0	disable distance report message (**default**)
n = 1	enable distance report message for PANIC, MPANIC and FPANIC

Note:

- This command does not work with range extenders.
- The message payload is DIST=NNN, where NNN is the distance in meters. NNN will be 020, 050, 100 or 999. 999 means the Pendant is out of range or the distance is over 100m.

Examples:

1. Enable distance report message :
   cmd wpan dist 1

   Example distance report:

```
$PPEN,0013A200407BCE71,97,DIST=020*2C
```

See also: [Down Pendant], [General Reports]

Firmware revision 2.0.5.2901

wpan panid *xxxx*

Set the WPAN PAN ID to communicate with the WPAN devices.

xxxx	WPAN PAN ID (hex digits) (**default 4465**)

Examples:

1. Change the WPAN PAN ID to 0x2000 :
   cmd wpan panid 2000
1. Query the current WPAN PAN ID :
   cmd wpan panid

See also: [Down Pendant]

Firmware revision 2.0.1.2221

wpan pensrv *x yyyy*

Configure the listening protocol and port of the Pendant Server that provides remote access to Man Down Pendant devices.

x = 0	UDP protocol (**default**)
x = 1	TCP protocol
yyyy = 0 to 65535	Port number of listening port, in decimal (**default 0**, disabled)

Examples:

1. Change the Pendant Server to listen on UDP port 21001 :
   cmd wpan pensrv 0 21001
1. Change the Pendant Server to listen on TCP port 21002 :
   cmd wpan pensrv 1 21002

See also: [Down Pendant]

Firmware revision 1.3.0.1718

wpan secure *n*

Secure access to the CTM-200's WPAN Pendant Server from the Internet.

n = 0	Allow direct access to WPAN Pendant Server from Internet (**default**)
n = 1	Secure - do not allow direct access to WPAN Pendant Server from Internet

Notes:

- If enabled, it will not be possible to remotely access the WPAN Pendant Server via the port specified in **wpan pensrv** and IP address allocated to the CTM-200 by the network.
- This feature can be used to support applications where the servers may be accessed through SSH tunneling.

Examples:

1. Set the CTM-200 to secure access to WPAN Pendant Server from Internet :
   cmd wpan secure 1

See also: [Down Pendant]

Firmware revision 1.3.0.2090

wpan stm *n*

Configure the CTM-200 to use the internal WPAN Gateway

n = 0	do not use internal WPAN Gateway (**default**)
n = 1	use internal WPAN Gateway

Examples:

1. Set the CTM-200 use the internal WPAN gateway for WPAN accessories :
   cmd wpan stm 1

See also: [Down Pendant]

Firmware revision 2.0.1.2221

wpanpanid xxxx

Set the WPAN PAN ID to communicate with the WPAN devices.

xxxx WPAN PAN ID (hex digits)

Using **wpanpanid** without a PAN ID, queries the WPAN PAN ID currently configured in the Chameleon modem.

Example:

cmd wpanpanid 2000 change the WPAN PAN ID to 0x2000

cmd wpanpanid queries the current WPAN PAN ID

Note: A [cmd save] and a power cycle must occur for the new settings to take effect.